UNIVERSIDAD COMPLUTENSE DE MADRID

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO ADMINISTRATIVO

TESIS DOCTORAL

EL DERECHO AL OLVIDO DIGITAL

Memoria para optar al grado de Doctor

Presentada por

JULIA MUÑOZ-MACHADO CAÑAS

Director

Prof. Dr. D. Tomás Cano Campos

Madrid

©Julia Muñoz-Machado Cañas, 2020

EL DERECHO AL OLVIDO DIGITAL

JULIA MUÑOZ-MACHADO CAÑAS

Departamento de Derecho Administrativo
Facultad de Derecho
Universidad Complutense de Madrid

Director
Prof. Dr. D. Tomás Cano Campos

Si tú me olvidas

"Si de pronto
me olvidas
no me busques,
que ya te habré olvidado"

Los versos del capitán- Pablo NERUDA, 1952

A mi buen padre.

A Borja y a nuestros tres hijos, Juan, Isabel y Santiago.

ÍNDICE

ABREVIATURAS

ACPD- Autoridad Catalana de Protección de Datos

AEPD- Agencia Española de Protección de Datos

AMPD- Agencia Madrileña de Protección de Datos

AN- Audiencia Nacional

Art.- Artículo

Art. 29 WG- Grupo de trabajo del artículo 29

AVPD- Agencia Vasca de Protección de Datos

CAM- Comunidad Autónoma de Madrid

CC- Código Civil

CDFUE- Carta de derechos fundamentales de la Unión Europea

CE- Constitución Española

/CE.- Comisión Europea

CEDH.- Convención Europea de los Derechos Humanos

CENDOJ- Centro de documentación judicial

CFC- Comisión Federal del Comercio

CJUE- Corte de Justicia de la Unión Europea ó TJUE

CNIL- Commission Nationale de l'Informatique et des Libertés (Francia)

CNPD- Comissão Nacional de Protecção de dados (Portugal)

COPPA.- Children's Online Privacy Protection Rule

CP- Código Penal

CTPDA- Consejo de transparencia y protección de datos de Andalucía

DEJ- Diccionario del español jurídico RAE

DGPDP- Dirección General de Protección de datos del Perú

DOCE- Diario oficial Comunidad Europea

Ed.- Editorial

EE.UU.- Estados Unidos

EM- Estados miembros

FAPE- Federación de asociaciones de periodistas de España.

FB- Facebook

ISSN- International Standard Serial Number / Número Internacional Normalizado de Publicaciones Seriadas

LGT- Ley 9/2014, general de Telecomunicaciones

LO- Ley Orgánica

LOPD- Ley Orgánica 15/1999, de protección de datos de carácter personal

LOPDGDD- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

LORTAD- Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal.

LPDP- Ley de protección de datos del Perú

LRJAP- Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

LSSI- Ley 34/2002, de servicios de la sociedad de la información.

NATO/OTAN- North Atlantic Treaty Organization; Organización del Tratado del Atlántico Norte

PE-Parlamento Europeo

P.O.-Procedimiento ordinario

PYME- Pequeña y mediana empresa

RAE- Real Academia Española de la Lengua

REDA- Revista Española de Derecho Administrativo

ReDCE- Revista de Derecho constitucional europeo

RGDA- Revista General de Derecho Administrativo

RGDC- Revista General de Derecho Constitucional

RGDE-Revista General de Derecho Europeo

RGPD- Reglamento General de protección de datos de la Unión Europea

STC- Sentencia del Tribunal Constitucional

STJUE- Sentencia del Tribunal de Justicia de la Unión Europea

SUPD- Supervisor Europeo de Protección de datos

TC- Tribunal Constitucional

TCE.- Tratado de la Comunidad Europea

TEDH- Tribunal Europeo de Derechos Humanos

TFUE.- Tratado de funcionamiento de la Unión Europea

TIC'S.- Tecnologías de la comunicación y de la información.

TJUE- Tribunal de Justicia de la Unión Europea ó CJUE

TS- Tribunal Supremo

UCLA- Universidad de California Los Ángeles

UE- Unión Europea

URL- Uniform Resource Locator

VV.AA.- Varios autores

WSJ.- Wall Street Journal

www.- world wide web

AGRADECIMIENTOS

Agradezco al Prof. Dr. D. TOMÁS CANO CAMPOS, haberse tomado el tiempo de enseñarme, atenderme y ayudarme como Tutor y Director de este trabajo de tesis. Gracias por tu paciencia infinita y tu dedicación sin las que seguramente no habría logrado mis objetivos.

A mi promoción en la ESCUELA DE DOCTORADO UCM, y particularmente a MERCEDES MOLINA, por el apoyo recibido y los ánimos recíprocos.

A los integrantes de MUÑOZ MACHADO ABOGADOS, colegas de Despacho, por su flexibilidad durante el tiempo de redacción de este trabajo, su cobertura en ocasiones y su compañerismo.

A mi familia y a mis amigos. A CRISTINA GONZÁLEZ ALONSO y a MARÍA ALBA SANTAMARÍA por ayudarme con la cuenta atrás.

A mi padre, SANTIAGO MUÑOZ MACHADO, por su ejemplo de estudio y trabajo infinitos.

A todos, ¡MUCHAS GRACIAS!

RESUMEN

El presente trabajo de investigación, titulado "El derecho al olvido digital", tiene como objeto el estudio de ese derecho, su emergencia y sus perfiles, así como el reto que el mismo supone para quienes ejercitan las libertades informativas en la nueva sociedad digitalizada en la que vivimos.

Resulta imperativo comenzar el desarrollo de esa investigación dedicando la primera parte del trabajo a analizar el nacimiento, alcance y contenido del derecho fundamental a la intimidad personal y familiar como antecedente del también derecho fundamental a la autodeterminación informativa.

Seguidamente, se procede al estudio detallado del derecho denominado "al olvido digital": los antecedentes de ese derecho en la legislación comunitaria y en la española hasta su reconocimiento positivo en el ordenamiento de la Unión Europea a través del Reglamento General de protección de datos (RGPD), que entró en vigor en la primavera de 2018, así como la reforma de la normativa española en materia de protección de datos que se ha producido con posterioridad a la entrada en vigor del RGPD.

Será objeto de examen y exposición detallada el papel fundamental que en el reconocimiento de ese derecho han tenido tanto la Agencia Española de Protección de Datos como el Tribunal de Justicia de la Unión Europea a través de la relevante Sentencia *Google c. España*, realizando asimismo el análisis pormenorizado de los pronunciamientos contenidos en esa resolución judicial, y una exposición de como los mismos se han visto reflejados en los posteriores pronunciamientos de los Tribunales nacionales: Audiencia Nacional, y posturas del Tribunal Supremo y, finalmente, Tribunal Constitucional en España (STC 58/2018).

Abordaremos también el diferente enfoque que sobre la materia han realizado los distintos órdenes jurisdiccionales españoles (civil/contencioso), destacando la discrepancia entre ellos sobre la responsabilidad, o no, del representante en España del motor de búsqueda. Hasta llegar al reconocimiento jurisprudencial del derecho al olvido incluso por parte de nuestro Tribunal Constitucional, mediante la Sentencia de 4 de junio de 2018, a la que ya hemos aludido en el párrafo precedente.

Serán también objeto de atención los distintos pronunciamientos tanto de la Agencia Española de Protección de Datos en materia de derecho fundamental al olvido digital, como otros del Tribunal Europeo de Derechos Humanos en materia de protección de datos, relevantes para la mejor comprensión de la materia. Se estudia en el Capítulo 4 la Sentencia del TEDH en la que se produce el primer pronunciamiento relativo al derecho al olvido digital (M.L y W.W c./ Alemania, de 28 de junio de 2018).

Igualmente se analizará el tradicional conflicto entre los derechos a la libertad de expresión e información desde la nueva óptica del derecho al olvido y el de la protección de datos de carácter personal, que no deja de ser una variable más en el estudio de ese choque y que debe considerarse en el balance que haya de hacerse respecto de la prevalencia de uno de ellos en el escenario de colisión de esos derechos.

Continuará el trabajo con la formulación de un análisis comparado de la paulatina implantación de ese derecho tanto en el ordenamiento de los países que integran la Unión Europea como en el de Estados terceros (EEUU, Canadá, Centro y Sudamérica, Japón, China o Australia son ejemplos), y que evidencian que las soluciones alcanzadas en Europa se van implantando progresivamente en el resto de ordenamientos de países terceros, por ser la comunitaria una de las normativas y jurisprudencia más avanzadas en el mundo en materia de protección de datos.

Termina el trabajo con las obligadas conclusiones y la referencia de la bibliografía utilizada.

ABSTRACT

This research paper, entitled, "The right to be forgotten", is intended as a study of the so-called "right to digital oblivion", and examines both, the processes by which this right came to be recognized and its diverse interpretations around the world, as well as the challenges that it poses for those who exercise informational freedoms in the Internet age.

In order to understand the vast scope and implications of the "right to digital oblivion", we must first analyse the concept of the fundamental right to privacy as a precedent of the fundamental right to data protection. This analysis will comprise the first section of the research paper.

The study follows with a second section (and primary focus of the paper) devoted to a detailed study of the "right to be forgotten". We will examine both the antecedents of said right in European and Spanish legislation prior to its codification in EU Law through the General Regulation of Data Protection (GRDP- entering into force last spring 2018), as well as the multiple reforms of Spanish regulations on data protection that have occurred after the codification of the GRDP.

The fundamental role that the Spanish Data Protection Agency and the Court of Justice of the European Union have had in the acknowledgment of this right will be subject to examination and detailed exposition through the study of the relevant judicial case "Google vs. Spain". We will conduct a detailed analysis of the pronouncements contained in that judicial decision, as well as an exposition of how this precedent has been reflected in the subsequent pronouncements of the Spanish Audiencia Nacional, and finally the implications for pronouncements made by the Spanish Supreme Court and Constitutional Court.

We will also discuss the different approaches that various Spanish courts (civil/administrative) have taken on the matter, highlighting the discrepancy between jurisdictions regarding the legal responsibility attributable to Google in Spain. This will include the jurisprudential recognition of the "right to be forgotten" by the Spanish Constitutional Court in the Judgment of June 4th, 2018.

The different pronouncements regarding the fundamental right to be forgotten made by both the Spanish Agency for Data Protection and the European Court of Human Rights will also be a focal point of the study. Of special interest is the ECHR Ruling containing the first pronouncement regarding the "right to be forgotten" (M.L and W.W v./ Germany, 28th June 2018), studied in Chapter 4.

We will also focus on the traditional conflict between the right to freedom of expression and information and the fundamental right to privacy. This will be analysed from the perspective of the right to be forgotten and its implications for data protection, which is another important variable that must be considered when attempting to find a just balance in the scenario of a conflict between these fundamental rights.

The central section of our study will conclude with a comparative analysis of the implementation of this right in a global context: on the one hand, the interpretation of the "right to be forgotten" by member states of the European Union, on the other, the interpretation of this right by third countries (USA, Canada, Central and South America, Japan, China or Australia are examples). This comparative study will show how the solutions achieved in Europe are gradually being introduced in other legal systems around the world, due to the fact that the European regulation on data protection are some of the most advanced in the world.

The research paper ends with conclusions, followed by bibliographical references.

INTRODUCCIÓN

A./ Motivación del presente trabajo de investigación:

El objeto de la presente tesis doctoral, "El derecho al olvido digital", tiene su origen en el interés, profesional y personal, de la doctoranda por el tradicional conflicto entre los derechos del art. 18 y 20 CE, que enfrentan a los derechos fundamentales al honor, intimidad personal y familiar y propia imagen con las libertades informativas.

Estudiando pormenorizadamente ese usual conflicto, se detectó como muchos de los postulados contenidos en la doctrina de nuestros Altos Tribunales para la resolución de ese problema se iban trasladando paulatinamente también al ámbito de la protección de datos en aquellos asuntos en los que se invocaba ese derecho fundamental a la protección de datos de carácter digital (18.4 CE) por estar involucrados en ellos medios de comunicación digitales.

Ese primer reflejo, que se produce en resoluciones de la Agencia Española de Protección de Datos (que este año cumple 25 años desde su creación, en 1994), respondía a denuncias de particulares en relación con ese tipo de conflictos, que eran confirmadas por nuestros tribunales, que adoptaban esos postulados de la Agencia, produciéndose en último término el reconocimiento normativo.

A esa línea de observación y trabajo, se sumó el dictado paralelo de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), *Google c./ España*, de 13 de mayo de 2014 (hace ahora cinco años), que consolidó la línea de trabajo anterior de la AEPD y que sin duda ha constituido uno de los pronunciamientos judiciales con mayor repercusión social de los últimos tiempos, y también con mayor incidencia en los distintos ordenamientos jurídicos.

El fallo de esa Sentencia determinó que el *derecho al olvido digital* quedase finalmente reconocido positivamente en el ordenamiento comunitario a través del art. 17 del Reglamento (UE) 2016/679), de 27 de abril de 2016, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos o RGPD), artículo que, a pesar de aplicarse de forma directa en todos los Estados miembros de la Unión Europea, también ha desencadenado una oleada de reformas en los ordenamientos de protección de datos de los distintos Estados miembros de la UE, precisamente para adaptarlos a las novedades de ese texto normativo comunitario.

Además, esa *Sentencia Google* ayudó a que los postulados relativos a la interpretación del tradicional choque entre los artículos 18 y 20 CE, aplicados al ámbito digital, se incorporasen también en muchos otros pronunciamientos judiciales no solo europeos, sino de todas partes del globo, ayudando a generalizar el tratamiento que, desde hace muchos años, venía aplicando la AEPD, pionera en la resolución de este tipo de conflictos.

A raíz del fallo del TJUE en la Sentencia *Google c. España*, tanto las agencias con competencia administrativa para la resolución de conflictos en materia de protección de datos como nuestros órganos judiciales nacionales han tenido que conocer de asuntos vinculados al alcance de ese derecho "a ser olvidado", estimando -o rechazando- las reclamaciones de particulares respecto de la necesidad, o no, de desindexar los resultados que arrojaban las búsquedas efectuadas con su nombre y apellidos en los motores de búsqueda de Internet.

Una corriente nueva que ha desembocado en un decisivo y reciente pronunciamiento de nuestro Tribunal Constitucional (4 de julio de 2018), reconociendo por primera vez en nuestro país a ese derecho al olvido rango de derecho constitucional, así como

al primer pronunciamiento que, de forma prácticamente coetánea (junio 2018), se produjo por parte del Tribunal Europeo de Derechos Humanos.

B./ Contenido del trabajo:

Ya se ha dicho que el objeto del presente trabajo de tesis es indagar en el origen de ese derecho de supresión de datos de carácter personal, "poéticamente" denominado "derecho al olvido", que sin duda se encuentran en el derecho fundamental a la intimidad personal y familiar, en su aplicación al mundo digitalizado en el que en la actualidad vivimos.

De ese derecho fundamental a la intimidad derivó el posterior reconocimiento del denominado derecho a la *autodeterminación informativa* (o derecho a la protección de datos de carácter personal), del que a su vez el derecho al olvido ha constituido una ramificación, adaptación, evolución o avance de sus postulados al sentido de los tiempos. A esos antecedentes dedicamos el Capítulo 1 de este trabajo, que constituyen a su vez su primera parte.

Seguidamente, se ha trabajado en un segundo bloque dedicado de forma íntegra al estudio del derecho al olvido digital. Esa segunda parte del trabajo está constituida por los Capítulos 2 a 6.

En esos capítulos se centran nuestros esfuerzos por rastrear el germen de ese derecho al olvido digital, tanto en la legislación comunitaria como en la nacional, que es el objeto del Capítulo 2 de esta memoria. En él nos detenemos en la exposición y análisis de las primeras normas en las que, primero de forma más tangencial y posteriormente más principal, se fue recogiendo y reconociendo el derecho a la protección de datos, en la legislación comunitaria y en la nacional, hasta desembocar en el reiterado derecho al olvido.

En ese Capítulo exponemos el proceso de gestación del derecho al olvido digital en Europa, comenzando por su antecedente más antiguo, que puede encontrarse en el Convenio 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de sus datos firmado en 1981, pasando por la introducción del derecho a la protección de datos en los Tratados fundacionales de la Unión Europea, y su posterior reconocimiento en su Carta de derechos fundamentales.

En el marco del desarrollo de las políticas de la Unión, esos principios generales se fueron implantando, en primer lugar, a través de la Directiva 95/46/CE y, paralelamente en nuestra legislación nacional, a través de su correspondiente transposición. Se analizan también en el citado Capítulo 2 los antecedentes normativos de la actual LOPD (la LORTAD), su desarrollo reglamentario a través del RD 1720/2007, y la normativa autonómica en materia de protección de datos (Madrid, Cataluña, País Vasco y Andalucía) y otras normas sectoriales con incidencia en el ámbito de la protección de datos.

El Capítulo 3, se dedica a analizar el contenido de la Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014 en el asunto C- 131/12, en el procedimiento entre Google España, S. L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González y su impacto. Particularmente, se exponen los antecedentes del supuesto sometido a la decisión de la AEPD que posteriormente dio lugar al recurso contencioso-administrativo ante la Sala tercera de la Audiencia Nacional en cuyo seno se produjo el planteamiento de las cuestiones prejudiciales que determinaron el fallo del TJUE (relativas a si la actividad de los motores de búsqueda constituye o no tratamiento, al ámbito de aplicación de la norma y finalmente sobre el alcance del derecho de cancelación), así como el contenido de ese fallo.

A continuación, se explica el impacto de esa Sentencia tanto en el marco de la Unión Europea (con el dictado de las directrices del Grupo de trabajo del art. 29 y la creación, por parte de Google, de un Consejo de expertos que publicaron orientaciones que pretendían guiar al gigante de Internet en la aplicación práctica de los pronunciamientos de la Sentencia a las miles de solicitudes de desindexación que se recibirán a partir de entonces), y seguidamente su impacto en España.

Respecto de la aplicación en España, se analiza el sentido del fallo de la Sentencia de la Audiencia Nacional a la recepción de la respuesta de las cuestiones prejudiciales planteadas ante el TJUE, el sentido del recurso de casación planteado por Google España, y el fallo de la Sala de lo contencioso-administrativo del Tribunal Supremo, que estima parcialmente ese recurso (Sentencia de la Sección 6ª de la Sala de lo contencioso-administrativo del Tribunal Supremo, núm. 1611/2016 de 4 julio), únicamente en cuanto a la delimitación de la legitimación pasiva de Google España respecto de Google Inc. Finalmente se plantean algunos interrogantes sobre la aplicación del contenido práctico de esa Sentencia, como por ejemplo qué pasará si los resultados que vulneran los derechos fundamentales del interesado no son consecuencia de una búsqueda por su nombre y apellidos sino de otro tipo de identificación, como por ejemplo un pseudónimo o apodo, u otros interrogantes prácticos aún sin resolver.

En el Capítulo 4, y bajo la rúbrica "la recepción de la doctrina del derecho olvido por los Tribunales nacionales y por el Tribunal Europeo de Derechos Humanos", se expone la forma en la que se ha recibido esa doctrina por los Tribunales nacionales, así como su impacto en el tradicional conflicto que ha enfrentado los derechos de los arts. 18 y 20 CE, y como ha intervenido recientemente en los mismos un "cuarto jugador", que sería el derecho a la protección de datos de carácter personal, al tratarse de publicación de noticias en medios digitales.

En particular, se analiza el contenido de la Sentencia del Pleno de la Sala de lo civil del Tribunal Supremo de 15 de octubre de 2015, dictada en el recurso de casación núm. 2772/2013, en la que se resuelve por esa Sala, por primera vez, el tratamiento que debe darse al denominado "derecho al olvido digital" en caso de conflicto con el derecho a la libertad de información, así como el contenido de la Sentencia del Tribunal Constitucional, de 4 de junio de 2018, dictada en el recurso de amparo 2096/2016, formulado frente a la Sentencia del TS que venimos de mencionar, y en el que el Tribunal Constitucional español reconoce por vez primera estatus de derecho fundamental al derecho al olvido digital, constituyendo un hito para el establecimiento y reconocimiento de ese derecho en nuestra jurisprudencia constitucional.

Finaliza ese Capítulo cuarto exponiendo y analizando el contenido de la también primera Sentencia del Tribunal Europeo de Derechos Humanos en materia de olvido digital, dictada en junio de 2018.

En el Capítulo 5, retomamos la regulación positiva del Derecho al olvido tanto en la legislación comunitaria como en la nacional, partiendo de los trabajos de modernización y adaptación de la reiterada Directiva 95/46/CE al nuevo contexto social, hasta la aprobación final del Reglamento General de protección de datos, texto que constituye sin duda el más importante avance normativo en materia de la protección de datos de las últimas décadas.

El citado RGPD reconoce por primera vez, en su artículo 17, el "derecho a la supresión de datos" o "al olvido digital", cuyo contenido y alcance se analiza también en el aludido Capítulo 2, derecho que tiene también un muy relevante impacto en todas las normativas de protección de datos de los Estados miembros de la UE.

También nos referimos en ese mismo Capítulo, al paquete legislativo para la reforma de la protección de datos impulsado por el legislador comunitario en 2018, finalizando con la exposición de la actualización de la normativa nacionl en materia de protección

de datos en España, hasta llegar a la actual Ley Orgánica de protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, *de protección de datos personales y garantía de los derechos digitales*), de reciente aprobación, en la que también se reconoce de forma positiva y por primera vez en nuestro ordenamiento el derecho al olvido digital desde una doble vertiente: el derecho a ser desindexado de los buscadores de Internet, y el de recuperar los datos facilitados a los responsables gestores de redes sociales, particularmente si los interesados en la recuperación de esos datos son menores de edad.

En el último Capítulo del trabajo (Capítulo 6), recogemos datos relativos a las resoluciones más relevantes de la AEPD en materia de protección de datos [incremento del número de reclamaciones desde la creación de la AEPD y hasta el día de hoy, análisis del sentido de esas resoluciones, y hemos procedido al análisis del contenido de las más recientes (las dictadas en el año 2019)], así como un acercamiento al sentido de las resoluciones de la Audiencia Nacional en aquéllos supuestos en que las mismas se han recurrido por los reclamantes/denunciados ante la Sala tercera de esa Audiencia Nacional. Así como también el análisis sobre el reconocimiento del derecho al olvido digital en distintos países de nuestro entorno comunitario, casi todos ellos a resultas del dictado de la *Sentencia Google* o de la aplicación del RGPD. Son ejemplos Francia, Italia, Alemania, Bélgica, Suecia, Reino Unido y Portugal. Finalmente, se aborda al reconocimiento de ese mismo derecho en estados terceros y ajenos a nuestro entorno comunitario, como es el caso de EE.UU, Canadá, Centroamérica y América del Sur, Rusia, Japón, China y Australia. En esa exposición, destaca el muy distinto análisis desde el cual el problema se aborda en EE.UU. desde la perspectiva de su radical incompatibilidad con el derecho a la libertad de expresión e información, reconocidos en la primera enmienda.

La investigación desarrollada se completa con una exposición de las conclusiones alcanzadas respecto de esos seis capítulos, abreviaturas y compilación de la bibliografía y recursos utilizados (legislación, jurisprudencia, resoluciones, dictámenes, informes y noticias de prensa).

C./ Metodología:

Los métodos de investigación utilizados han sido varios, pero fundamentalmente, y considerando el contenido jurídico de la materia objeto de estudio, los más empleados han sido el histórico, exegético, dogmático y comparado. Y ello porque una buena parte del trabajo se ha dedicado al estudio del nacimiento de ese derecho, al análisis del contenido de la normativa española y comunitaria en materia de protección de datos, y el contexto histórico y social en el que dichas normas se promulgaron.

Asimismo ha sido preciso emplear en la presente investigación los métodos exegético y dogmático, por haber sido necesario analizar el contenido propio de las normas en función de la significación de los términos que en las mismas se emplean, o abstraerse en ocasiones de esa significación literal, para considerar las aportaciones e interpretaciones doctrinales al respecto, considerando que, también es posible encontrar conclusiones contrapuestas en relación a un determinado asunto dependiendo de cuál sea el parecer de los estudiosos en relación al mismo (sobre este particular, es significativo el distinto enfoque que sobre la materia del derecho al olvido realizan el ordenamiento norteamericano en contraposición al europeo, por ejemplo).

Ya hemos dicho como, tratándose de una investigación jurídica realizada en el ámbito del derecho constitucional y del derecho público nacional y comparado, ha sido preciso:

- Analizar tanto el ordenamiento jurídico nacional como el comunitario en el ámbito de: 1) los derechos fundamentales en general; 2) el derecho fundamental a la intimidad; 3) el derecho a la autodeterminación informativa; 4) el derecho al olvido.

- La lectura y estudio de trabajos preparatorios de esas normas, y particularmente los relativos a la tramitación del RGPD y la nueva LOPDDD, que han sido especialmente ilustrativos respecto de la motivación y objetivos para su promulgación, y que normalmente se completan con consultas públicas, informes de impacto, sondeos de opinión, revisión del grado de trasposición de las normas, etc.

- Además, tratándose en el presente caso del estudio de un derecho en cuya gestación y asentamiento ha tenido un papel capital la jurisprudencia comunitaria y constitucional, ha resultado también muy relevante para la exposición del asunto objeto de análisis la lectura y estudio de la jurisprudencia nacional y comunitaria tanto en el ámbito del derecho fundamental a la intimidad, como en el del derecho a la autodeterminación informativa y posteriormente del derecho al olvido digital. Respeto de este último, ha resultado especialmente relevante el análisis de las Sentencias referidas al derecho al olvido, tanto en el ámbito europeo, con en el nacional, tanto en el ámbito administrativo como en el civil, y la comparación de los resultados, no siempre idénticos, alcanzados en los distintos órdenes jurisdiccionales.

- En los mismos términos, ha resultado interesante el análisis del contenido de las resoluciones, informes y demás documentos emitidos por las agencias reguladoras en la materia objeto de estudio en este trabajo de tesis (Grupo de trabajo del art. 29; Agencia Española de Protección de Datos; Agencias autonómicas de protección de datos, etc.).

- Todo ello combinado con el estudio de los dictámenes e informes emitidos por las Instituciones con competencia en materia de protección de datos, análisis de las aportaciones de los distintos autores: lectura de monografías y artículos de revistas vinculados al tema seleccionado, así como de artículos de prensa en los que quedan reflejados los asuntos de mayor actualidad.

El empleo de todos esos medios me ha permitido ir desengranando y reflejando en el presente trabajo la implantación paulatina del derecho al olvido en nuestro entorno comunitario y nacional, así como el otros Estados ajenos a ese ámbito geográfico, las posiciones de la doctrina al respecto, y la manera en la que se han enfrentado también a este nuevo problema tanto nuestros tribunales de justicia como las agencias con competencia para abordarlos.

D./ Bibliografía y recursos empleados:

Hemos utilizado para el estudio, elaboración y redacción del presente trabajo una muy abundante bibliografía, que abarca desde la lectura y estudio de los "clásicos" doctrinales de los derechos fundamentales y del derecho fundamental a la intimidad, hasta la de aquellos autores que estudiaron por vez primera el derecho a la determinación informativa hasta terminar con la lectura de aquéllos otros que están estudiando y escribiendo actualmente sobre el derecho al olvido digital (son menos).

Al margen de esas lecturas, ya hemos indicado como hemos manejado también las normas, sentencias y resoluciones más modernas y relevantes en la materia, junto con los informes, consultas públicas, encuestas, y otros trabajos consultivos llevados a cabo tanto por las Instituciones Europeas como por las sociedades mercantiles del sector, organismos reguladores y expertos.

El detalle de todos los recursos utilizados (incluidos los artículos de prensa) puede encontrarse, convenientemente ordenado en el Capítulo "Bibliografía", y siguiendo el siguiente esquema: 1) libros; 2) artículos; 3) legislación; 4) jurisprudencia; 5) informes, consultas públicas, conferencias y dictámenes; y finalmente, 6) artículos de prensa.

CAPÍTULO 1

DE LA INTIMIDAD AL OLVIDO.

SUMARIO: 1.1. CONCEPCIÓN GENERAL DE LOS DERECHOS FUNDAMENTALES; 1.2. LAS PRIMERAS FORMULACIONES DOCTRINALES DEL DERECHO FUNDAMENTAL A LA INTIMIDAD; 1.2.1. "THE RIGHT TO PRIVACY" DE WARREN Y BRANDEIS; 1.2.2.LA SISTEMATIZACIÓN DE PROSSER; 1.2.3. OTRAS TEORÍAS ALREDEDOR DEL DERECHO FUNDAMENTAL A LA INTIMIDAD; 1.3. RECONOCIMIENTO DEL DERECHO FUNDAMENTAL A LA INTIMIDAD EN LOS CONVENIOS INTERNACIONALES; 1.4. EL CONTENIDO Y ALCANCE DEL DERECHO FUNDAMENTAL A LA INTIMIDAD EN EL CEDH; 1.5. EL ART. 18 DE LA CONSTITUCIÓN ESPAÑOLA; 1.6. EL DERECHO FUNDAMENTAL A LA INTIMIDAD EN LA JURISPRUDENCIA CONSTITUCIONAL; 1.7. LOS NUEVOS RETOS JURÍDICOS DEL DERECHO FUNDAMENTAL A LA INTIMIDAD; 1.7.1. INTERNET Y DERECHO A LA INTIMIDAD; 1.7.2. TRATAMIENTO DE DATOS E INTIMIDAD; 1.7.3. ECONOMÍA DE DATOS E INTIMIDAD; 1.7.4. REDES SOCIALES: DE LA INTIMIDAD A LA "EXTIMIDAD"

1.1 Concepción general de los derechos fundamentales

El Tribunal Constitucional español conceptualiza y define los derechos fundamentales como "derechos subjetivos, derechos de los individuos no solo en cuanto derechos de los ciudadanos en sentido estricto, sino en cuanto garantizan un status jurídico o la libertad en un ámbito de la existencia" y que "al propio tiempo, son elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado social de Derecho o el Estado social y democrático de Derecho, según la fórmula de nuestra Constitución (art. 1.1)"[1].

[1] Sentencia 25/1981, de 14 de julio; (BOE núm. 193, de 13 de agosto de 1981) https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/25

Los autores más destacados[2] subrayan que la definición del concepto "derechos fundamentales" puede abordarse desde una perspectiva ostensiva (por *denotación* o *extensión* "mostrando ejemplos de objetos o cosas de los que puede predicarse que son o que tienen que ver con los derechos humanos") o desde la perspectiva del análisis lógico (consistente en un análisis "tendente a establecer la comprensión, intensión o connotación de los derechos humanos a partir de sus notas constitutivas").

Se señala también por la mayoría de la doctrina que los derechos humanos nacen con vocación individualista y, que esas libertades individuales, reconocidas en origen, vienen a configurar la que se denomina «primera fase o generación» de los derechos humanos.

En Europa, los primeros textos en los que se determinó que debía considerarse en tal condición ("derecho humano") fueron la "Petition of Right"[3] y el "Bill of Rights"[4] ingleses de principios y finales del siglo XVII, en los que se plasmó una idea más integral de lo que debe ser considerado como tales "derechos humanos".

Esos primeros textos normativos fueron posteriormente ejemplo para otros ulteriores, como los que resultaron de las revoluciones norteamericanas y francesas del siglo XVIII: la Declaración de Independencia Norteamericana[5], la Declaración de Derechos del buen pueblo de Virginia de 1776[6] y la Declaración Francesa de los

[2] Son ejemplos: DIEZ-PICAZO, L.M.: *Sistema de derechos fundamentales*, 4ª Ed. Civitas, Madrid, 2013, la extensa obra MARTÍN-RETORTILLO, L. (por ejemplo: *Los derechos fundamentales y la constitución*, Ed. El Justicia de Aragón, Zaragoza 2009) ó PÉREZ LUÑO, A.E.: *Concepto y concepción de los derechos humanos*, Doxa. Cuadernos de Filosofía del Derecho. Núm. 4, 1987.
[3] *Petition of Rights*, 7/6/1628 en PECES-BARBA MARTÍNEZ, G.: *Derecho positivo de los derechos humanos*, Madrid, Debate, 1985, págs. 62-65.
[4] Publicada en 1689, el texto puede consultarse en: https://www.parliament.uk/about/living-heritage/evolutionofparliament/parliamentaryauthority/revolution/collections1/collections-glorious-revolution/billofrights/
[5] http://hmc.uchbud.es/Materiales/DeclaraUSA.pdf
[6] Declaración de derechos del buen pueblo de Virginia, 12 de junio 1776, en PECES-BARBA MARTÍNEZ, Op. cit. 3

Derechos del Hombre y del Ciudadano en el año 1789[7]. Esta última Declaración recogió un importantísimo conjunto de principios enunciados en tan solo 17 artículos, que hoy son considerados esenciales para todas las sociedades civilizadas por ser ejemplo y compendio de las principales necesidades humanas a cubrir y proteger.

Esa primera hornada de derechos fue evolucionando a lo largo de todo el siglo XIX, determinando que esos primeros catálogos de derechos y libertades se fueran completando con una segunda oleada (o segunda generación), constituida a su vez por derechos de carácter económico, social y cultural que se consagran con la sustitución del Estado liberal de Derecho por el Estado social de Derecho[8].

La distinción entre ambas generaciones de derechos (primera y segunda) supone que los derechos humanos vengan considerados en la primera de esas dos generaciones como derechos de defensa de las libertades del individuo que exigen la autolimitación y la no injerencia de los poderes públicos en la esfera privada y se tutelan por su mera actitud pasiva y de vigilancia en términos de política administrativa. En la segunda (correspondiente a los derechos económicos, sociales y culturales), se traducen en derechos de participación, que requieren una política activa de los poderes públicos encaminada a garantizar su ejercicio y se realizan a través de las técnicas jurídicas de las prestaciones y los servicios públicos.

Posteriormente, se reconoció una "tercera generación" de derechos fundamentales, relacionados con asuntos tales como el derecho a la paz, a la cultura, las nuevas tecnologías, la conservación del medio ambiente o la protección de los consumidores.

Conviene subrayar, por tanto, que los derechos fundamentales van evolucionando y adaptándose a los nuevos retos que plantean al Derecho las cambiantes circunstancias

---

7 http://www.cervantesvirtual.com/obra-visor/declaracion-de-los-derechos-del-hombre-y-del-ciudadano/html/8b364e78-7358-11e1-b1fb-00163ebf5e63_1.html

8 También en PÉREZ LUÑO, ya citado.

históricas, sociales y políticas, que es lo que, al fin y al cabo, ha sucedido con el derecho fundamental a la intimidad, como seguidamente se verá.

1.2. Las primeras formulaciones doctrinales del derecho fundamental a la intimidad

Las primeras formulaciones doctrinales en las que se refleja el concepto de "derecho fundamental a la intimidad" son las de COOLEY[9] y WARREN Y BRANDEIS[10], quienes aludieron por primera vez, de forma respectiva, tanto al "right to be let alone" como al "right to privacy".

THOMAS L. COOLEY empleó la expresión "the right to be let alone" en la primera edición de su *Treatise on the Law of Torts*, publicada en 1879. En esa obra, COOLEY definía el "derecho individual a la inmunidad personal frente a agresiones físicas", entendido como "el derecho de la persona a la completa inmunidad" que definía como el derecho "a ser dejado solo". Al analizar el alcance de las violaciones de las Cuarta y Quinta enmienda en los casos de registros y requisas ilegales del domicilio con el objetivo de obtener pruebas suficientes para el procesamiento de los acusados, COOLEY afirmaba que el derecho de la persona a protegerse frente a invasiones de la privacidad alcanza "tanto frente a la intromisión ilegal de los agentes del gobierno" como "frente a la curiosidad lasciva del público en general".

Esa expresión acuñada por COOLEY reflejaba la máxima del *common law* "a man´s house as his castle" ("mi casa es mi castillo"), en virtud de la cual se garantizaba la protección del ciudadano en su domicilio frente a injerencias del Gobierno, salvo

[9] COOLEY, T.: *A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract*, Ed. Callaghan, Chicago 1879.
[10] WARREN, S. Y BRANDEIS, L.: "The Right to privacy", en *Harvard Law Review*, Vol. IV, 15 de diciembre de 1890, núm. 5.
http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

supuestos muy específicos. Argumentación que fue aceptada de forma expresa por el Tribunal Supremo de los Estados Unidos en el caso *Boyd vs. United States*[11], entre otros.

Once años después de esa primera formulación, la doctrina acuñada por COOLEY es desarrollada por SAMUEL D. WARREN y LOUIS D. BRANDEIS, quienes publicaron en la Harvard Law Review su célebre artículo "The Right to privacy"[12][13], publicación que se ha convertido en un "clásico de la literatura jurídica"[14]. Y ello, no solo por la novedad que supuso en su momento respecto de la formulación del derecho a la intimidad, sino también porque su contenido sigue teniendo en la actualidad plena vigencia, casi 130 años después de haberse publicado por primera vez.

1.2.1. "The right to privacy" de Warren y Brandeis

El artículo "The Right to privacy" de WARREN y BRANDEIS es uno de los más citados por la doctrina y jurisprudencia norteamericanas, motivo por el cual nos parece interesante dedicarle cierta atención en este trabajo, considerando su importancia y transcendencia en las formulaciones posteriores del derecho fundamental a la intimidad objeto de estudio.

Subraya la PROF. SALDAÑA[15], en un estudio profundo del citado artículo, que sus orígenes, según resulta del análisis de la correspondencia intercambiada por éstos con posterioridad a la redacción de esa publicación, sugieren que WARREN estaba muy

[11] U.S. Supreme Court; Boyd v. United States, 116 U.S. 616 (1886) https://supreme.justia.com/cases/federal/us/116/616/
[12] Op. cit. 10
[13] ARCE JARANIZ, A.: "El derecho de la intimidad. De Samuel D. Warren y Louis D. Brandeis", *Revista Española de Derecho Constitucional*, Año 16. Núm. 47. Mayo-Agosto 1996.
[14] Así lo califica el Prof. BENIGNO PENDÁS en la introducción que hizo de la obra en la versión publicada por Cuadernos CÍVITAS.
[15] SALDAÑA, M.N.: "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis". *Revista de Derecho Político de la UNED*, N.º 85, septiembre-diciembre 2012, págs. 195-240

enfadado con el trato que le había dispensado en su día la prensa sensacionalista[16], y que ese fue el motivo por el que sugirió a BRANDEIS[17] la redacción del ensayo.

Se trataba, por tanto, y a resultas de una situación vivida por uno de ellos, de reclamar resortes jurídicos que permitieran la defensa del individuo frente a las injerencias no queridas de la prensa, y particularmente de la publicación generalizada de aspectos íntimos de la vida privada. Resortes que no existían en el momento temporal en el que los dos autores escribieron su célebre artículo.

Del contenido de ese trabajo se infiere que los autores estaban preocupados y se sentían amenazados por los logros tecnológicos ("ingenios mecánicos", como los denominan en su artículo, que permiten, por ejemplo, "la toma subrepticia de fotografías" o el empleo del teléfono), así como por la deriva de la prensa, de quien temían "la difusión indiscriminada de información privada" "divulgándose los más íntimos detalles en las columnas de los periódicos para satisfacer la curiosidad lasciva mediante la intromisión en el ámbito privado".

El artículo subraya en uno de sus párrafos más reproducidos como "la intensidad y la complejidad de la vida, que acompañan a los avances de la civilización, han hecho necesario un cierto distanciamiento del mundo, y el hombre, bajo la refinada influencia de la cultura, se ha hecho más vulnerable a la publicidad, de modo que la soledad y la intimidad se han convertido en algo esencial para la persona; por ello, los nuevos métodos e inventos, al invadir su intimidad, le producen un sufrimiento espiritual y una angustia mucho mayor que la que le pueden causar los meros daños personales".

[16] Unas teorías apuntan a que fue objeto de la prensa amarilla de la época por motivo de su matrimonio con la hija de un Senador; otras, que fue la boda de su propia hija la que fue objeto de publicaciones y motivó su enfado y posterior redacción del artículo.
[17] Quien fue Juez de la Corte Federal desde 1916 a 1939, nombrado por el presidente Wilson.

Para dar respuesta a esas amenazas, los autores manifiestan la necesidad de "definir un principio que pueda ser debidamente invocado para amparar la intimidad de la persona y, en caso afirmativo, determinar la naturaleza y extensión de dicho amparo". Tal principio defendería al individuo "frente a la invasión de una prensa demasiado pujante, del fotógrafo, o del poseedor de cualquier otro moderno aparato de grabación o reproducción de imágenes y sonidos", que se materializa en el "derecho a la privacidad", confiriéndoles disponibilidad para decidir "hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos o emociones".

Los autores también hacen el ejercicio de diferenciar el derecho a la intimidad de los derechos a la libertad y a la propiedad, alcanzando el derecho a la intimidad la protección de ámbitos inmateriales e intereses espirituales de la persona, frente a la configuración tradicional del derecho a la propiedad, que garantiza la posesión sobre los bienes. Puntualizando seguidamente que "el principio que tutela los escritos personales y cualquier otra obra producto del espíritu o de las emociones es el derecho a la intimidad" y que "el derecho no necesita formular ningún principio nuevo cuando hace extensivo este amparo a la apariencia personal, a los dichos, a los hechos, y a las relaciones personales, domésticas o de otra clase". Derecho que sería extensible a la facultad de una persona física para impedir que su retrato circule (sería el reconocimiento del derecho fundamental a la propia imagen).

Se formulan seguidamente también ciertas limitaciones a este derecho a la intimidad, justificadas por los autores en la necesidad de que los derechos del individuo cedan ante "el bienestar general o la equidad" y que se adaptan de las previamente desarrolladas en la ley de difamación y libelo y en la ley de propiedad intelectual:

1. "El derecho a la intimidad no impide la publicación de aquello que es de interés público o general" (se señala por los autores, por ejemplo, que una misma información puede revestir, o no, carácter de información de interés para la

generalidad del público dependiendo de si la persona a quien alude esa información tiene o no interés público).

2. "El derecho a la intimidad no prohíbe la información sobre un tema, aun siendo éste de naturaleza privada, si la publicación se hace en las circunstancias en que, conforme a la ley de difamación y libelo, sería calificada de información privilegiada" (esto es, la que se realiza en sede judicial).

3. No hay derecho a reparación si la violación de la intimidad se hace de forma oral y sin causar daños.

4. El derecho a la intimidad del individuo decae con su consentimiento.

5. La veracidad de lo publicado no excluye la existencia de intromisión.

6. Tampoco es defensa la inexistencia de "malicia" en el autor de la publicación.

7. Se establecen algunos criterios para la reparación de los daños sufridos como consecuencia de esas intromisiones, estableciéndose la posibilidad de reconocer una compensación como sucede con las leyes de libelo. Se apunta la posibilidad de revestir este tipo de intromisiones de responsabilidad criminal, siendo para ello precisa la previa reforma legal.

Resulta ciertamente sorprendente la actualidad de todos esos postulados, que siguen siendo aplicables hoy en día, y que, en el caso español, han sido trasladados a nuestro ordenamiento tanto a través de las correspondientes normas como a través de la interpretación que los tribunales han hecho de las mismas.

Postulados que, con pocos matices, se vienen aplicando asimismo a los problemas suscitados por los "ingenios mecánicos" del S. XXI, que son Internet y sus motores

de búsqueda, los smartphones y todos esos aparatos a los que, posiblemente superando las expectativas de WARREN Y BRANDEIS (a quienes ya escandalizaban los más rudimentarios modelos de máquinas de fotos y el teléfono), debe hacer frente la sociedad contemporánea.

El artículo de WARREN Y BRANDEIS originó una preocupación colectiva por la protección de la esfera privada del individuo que vive en sociedad, que es respetuosa asimismo de la dimensión social o colectiva, estableciendo también límites sobre ese derecho en beneficio y cuidado del estado democrático.

1.2.2. Sistematización de Prosser

Ese artículo de Warren y Brandeis fue revisado y sistematizado posteriormente por WILLIAM L. PROSSER en 1960, mediante un artículo publicado en la California Law Review[18], en el que distinguía cuatro ámbitos de la vida privada susceptibles de ser vulnerados y atribuía a cada una de esas intromisiones una acción distinta para su protección. Serían: a) *introsion on an individual´s privacy* (intrusión en la privacidad individual); b) *public disclosure of private facts* (divulgación de hechos concretos de la vida privada); c) *putting an individual in a false light in the public eye* (difusión de informaciones falsas y oprobiosas); d) *appropiation of some elements o fan individual´s personality* (uso inconsentido de la imagen, voz u otros atributos del individuo).

1.2.3. Otras teorías alrededor del derecho fundamental a la intimidad

Además de la teorización de PROSSER, otros estudiosos han reflexionado sobre el alcance del derecho fundamental a la intimidad[19].

[18] PROSSER, W.: "Privacy", *California Law Review*, 1960.
[19] WESTIN, A.: *Privacy and freedom*, Ed. Atheneum, New York, 1967

Es el caso de la teoría de las esferas o círculos concéntricos ideada por HUBMANN[20] en 1953. La tesis de HUBMANN parte de la división de este derecho general de la personalidad en tres sectores o áreas de la intimidad, cada uno de los cuales constituye una esfera. Tenemos así en esta primera formulación tres campos de la intimidad: la esfera individual (privatsphäre), la esfera privada (vertravensphäre) y la esfera de secreto (gehimsphäre).

Esta teoría de las esferas fue recogida por HENKEL[21] y aplicada al ámbito penal, realizando algunos ajustes en la terminología y añadiendo otro espacio de protección entre la esfera privada y la esfera de secreto: la denominada esfera de confianza.

Criticando el carácter "separatista" de la Teoría de las esferas, MADRID CONESA[22] desarrolla la "teoría del mosaico", que niega que cualquier vivencia aisladamente considerada tenga valor o significado por sí misma, ya que ese valor solo podría alcanzarlo en combinación con otras que funcionarían del modo en el que lo hacen las teselas de un mosaico, dando aquí como fruto una perspectiva de la vida privada de cada persona atendiendo a sus particulares circunstancias, y considerando para ello pequeños fragmentos que abordan la vida privada del individuo desde distintas perspectivas, como sucede en un mosaico.

[20] HUBMANN, H: *Das Persönlichkeitsrecht*, 2, Auflage, Köln/Graz, Böhlau, 1967 (1ª edición, 1953), ps. 267 y ss.
[21] HENKEL: "Der Strafschutz des Privatlebens gegen indiskretion" en *Verhandlugen des Zweiundvierzigsteb Deutschen Juristentages*, Dusseldorf,1957, Tubingen, C,B.Mohr, 1959, p. 60 y ss
[22] MADRID CONESA, F.: *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984

1.3. Reconocimiento del derecho fundamental a la intimidad en los Convenios Internacionales

Descendiendo del campo de los conceptos al ámbito normativo, la Declaración Americana de Derechos y Deberes del Hombre[23], de 2 de mayo de 1948, aprobada por la IX Conferencia internacional americana realizada en Bogotá, es el primer texto que reconoce de forma positiva el derecho fundamental a la intimidad personal y familiar.

Particularmente, el art. 5 de la citada Declaración dispone que: "toda persona tiene derecho a la protección de la ley, contra los ataques abusivos a su honra, su reputación y su vida privada y familiar". Ese texto legislativo fue el primer acuerdo internacional sobre derechos humanos, anticipando la Declaración Universal de los Derechos Humanos, sancionada seis meses después.

Efectivamente, en diciembre de ese mismo año 1948, se promulgó la Declaración Universal de los Derechos Humanos[24], cuyo artículo 12 dispone que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene el derecho a la protección de la ley frente a tales ataques o injerencias." La Declaración Universal de los Derechos Humanos fue elaborada por representantes de todas las regiones del mundo con diferentes antecedentes jurídicos y culturales, y proclamada por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948 en su Resolución 217 A (III), como un ideal común para todos los pueblos y naciones. La Declaración establece, por primera vez, los derechos humanos fundamentales que deben protegerse en el mundo entero y ha sido traducida en más de 500 idiomas.

[23] http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp
[24] http://www.un.org/es/universal-declaration-human-rights/

Por su parte, y en el continente europeo, el Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales de 1950[25], reconoce este derecho en su artículo 8.1. "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". Los veintiocho Estados miembros de la Unión Europea son signatarios del Convenio. Además, la Carta de los derechos fundamentales de la Unión Europea afirma en su preámbulo que pretende reafirmar los derechos reconocidos por (entre otras fuentes) el Convenio y la jurisprudencia del Tribunal Europeo de Derechos Humanos. Su artículo 52 afirma que los derechos proclamados en la Carta y que tengan correspondencia en la Convención, tendrán, al menos, el mismo alcance que confiere esta última. El precepto se ve reafirmado por el artículo 53, que afirma que ninguna de las disposiciones de la Carta podrá interpretarse como limitativa de los derechos proclamados en la Convención.

Por su parte el Pacto internacional de los derechos civiles y políticos de 1966[26] lo reconoce en su artículo 17.1: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".

1.4. El contenido y alcance del derecho fundamental a la intimidad en el CEDH y la interpretación del TEDH

Venimos de señalar como el art. 8 del CEDH, bajo la rúbrica "Derecho al respeto a la vida privada y familiar", establece:

> *"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

[25] https://www.echr.coe.int/Documents/Convention_SPA.pdf
[26] *Pacto Internacional de Derechos Civiles y Políticos* adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966 https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás."*

El contenido de ese artículo es muy parecido al del art. 18 de nuestra Constitución Española, al que aludiremos un poco más adelante[27]. Su objetivo fundamental es "establecer determinadas zonas o ámbitos protegidos frente a cualquier injerencia exterior"[28].

Subraya la doctrina como el art. 8 del CEDH ofrece una protección más amplia que la del estricto derecho a la privacidad, y ello a pesar de que la Corte ha renunciado a realizar una definición cerrada del concepto "vida privada", incluyendo garantías de "autonomía personal" en sentido amplio, como lo es, por ejemplo, la identificación de género.

El concepto protegido por la CEDH en la interpretación que de su art. 8 ha hecho el TEDH comprende: la vida privada, la familia, la vida en el domicilio, la integridad física y moral, el honor y la reputación, la no revelación de hechos triviales, irrelevantes o vergonzantes, la publicación no autorizada de fotografías, protección de la información facilitada de manera confidencial, etc.

Además de los anteriores, que en líneas generales pueden entenderse también protegidos por nuestro ordenamiento en la redacción que en el mismo se ha dado al

[27] Infra apartado 1.5 del presente Capítulo 1.
[28] GARCÍA ROCA, J. y SANTOLAYA, P. (Coordinadores): *La Europa de los derechos. El convenio Europeo de Derechos Humanos*, Ed. Centro de Estudios Políticos y Constitucionales, 2ª Edición, Madrid, 2009.

art. 18 de la CE, hay otros aspectos de la vida familiar que difícilmente pueden entenderse comprendidos en "nuestra intimidad familiar", como son: el control de las medidas de tutela, adopción y visita, o las aplicaciones de ese derecho a la intimidad familiar a los extranjeros como son la reagrupación familiar y el establecimiento de límites a la expulsión como consecuencia del arraigo[29].

No en vano, el TEDH ha afirmado de forma expresa que "no considera posible, ni necesario, intentar definir de manera exhaustiva la noción de "vida privada", pero que sería excesivamente restrictivo limitarla a un "círculo íntimo" en que cada uno puede desarrollar su vida personal… y que debe incluir la posibilidad de mantener relaciones con sus semejantes". Así se refleja en el asunto *Niemietz contra Alemania*[30], de 16 de diciembre de 1992.

1.5. El art. 18 de la Constitución Española

La Constitución Española de 27 de diciembre de 1978 dedica su título I a los "derechos y deberes fundamentales", estableciéndose en la Sección 1ª del Capítulo II de ese Titulo primero, un haz de derechos que parten de los fundamentales a la vida y a la integridad física y moral (art. 15 CE), pasan por la libertad ideológica y religiosa (art. 16 CE), libertad, seguridad (art. 17 CE), etc. hasta llegar a los derechos a la educación (art. 27 CE), de huelga, sindicación (art. 28 CE), y otros de carácter laboral.

[29] SANTOLAYA, P: "El derecho a la vida privada y familiar (un contenido notablemente ampliado del derecho a la intimidad" en *La Europa de los derechos. El convenio Europeo de Derechos Humanos*, de SANTOLAYA, P., y GARCÍA ROCA, J. (Coordinadores): Ed. Centro de Estudios Políticos y Constitucionales, 2ª Edición, Madrid, 2009.
[30] Sentencia del TEDH *Niemietz contra Alemania* de 16 diciembre 1992, serie A núm. 251.

Explicamos en nuestro comentario al art. 18 de la CE (en la obra colectiva *Comentario mínimo a la Constitución Española*) como ese artículo[31] ampara distintos derechos, todos ellos inspirados en el fundamental a la intimidad, pero con perfiles propios: el derecho al honor, a la intimidad personal y familiar y a la propia imagen; la inviolabilidad del domicilio; el secreto de las telecomunicaciones, y el derecho fundamental a la protección de datos[32].

El derecho al honor ha gozado siempre de protección por parte de nuestro ordenamiento, configurándolo como uno de los derechos clásicos de la personalidad y ha sido objeto de una larga interpretación jurisprudencial. Consecuencia de esa interpretación, se distinguen un aspecto inmanente y otro trascendente del honor: "el primero consiste en la estima que cada persona tiene de sí misma"; el segundo, "radica en el reconocimiento de los demás de nuestra dignidad" (STS de 23 de marzo de 1987[33]). Se vincula al contexto social, y deben tenerse en cuenta en su valoración distintas circunstancias tales como la relevancia de la información difundida, la relevancia pública del personaje, su afectación a la vida profesional o a la privada, etc.

El derecho fundamental a la intimidad "tiene por objeto garantizar al individuo un ámbito reservado de su vida, excluido tanto del conocimiento como de las intromisiones de terceros" (STC 144/1999 de 22 de julio[34]). En cuanto derivación de la dignidad de la persona reconocida en el art. 10.1 CE, protege la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás,

---

[31] Ver, MUÑOZ-MACHADO CAÑAS, J.: "Comentario al art. 18 CE" en la obra colectiva *Comentario mínimo a la Constitución Española*, Dirigida por el Prof. Dr. D. SANTIAGO MUÑOZ MACHADO, Ed. Crítica, Madrid, 2018.

[32] Sobre el art. 18 de la CE ver también, RODRIGUEZ PIÑEIRO y BRAVO FERRER, M y CASAS BAAMONDE, M.E.: "Los derechos al honor, intimidad personal y propia imagen", págs. 511-529, "La protección de datos", págs. 562 a 566, *Comentarios a la Constitución Española; XL Aniversario,* , Ed. Fundación Wolters Kluwer, Boletín Oficial del Estado, Tribunal Constitucional y Ministerio de Justicia Madrid, 2018.

[33] Sentencia 23/1987, de 23 de febrero (BOE núm. 54, de 04 de marzo de 1987) http://hj.tribunalconstitucional.es/es/Resolucion/Show/755

[34] Sentencia 144/1999, de 22 de julio (BOE núm. 204, de 22 de agosto de 1999) http://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/1999/144

necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC nº 231/1988, de 2 de diciembre[35], 197/1991, de 17 de octubre[36]; 57/1994, de 18 de febrero[37]; 143/1994, de 9 de mayo[38]; 207/1996, de 16 de diciembre[39]; 156/2001, de 2 de julio[40]; 127/2003, de 30 de junio[41], 196/2004, de 15 de noviembre[42], entre otras).

Por su parte, el derecho fundamental a la propia imagen es un derecho de la personalidad estrechamente relacionados con el honor y la intimidad, pero autónomo (Sentencia del Tribunal Constitucional 81/2.001, de 26 de marzo[43]) y con contenido propio y específico (Sentencias del Tribunal Constitucional 156/2.001, de 2 de julio[44], y 83/2.002, de 22 de abril[45]). Entendiendo la imagen como la representación gráfica de la figura humana, visible y recognoscible, y el derecho a la imagen como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral de las personas, que atribuye a su titular un derecho a determinar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública

[35] Sentencia 231/1988, de 2 de diciembre (BOE núm. 307, de 23 de diciembre de 1988); http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1172
[36] Sentencia 197/1991, de 17 de octubre (BOE núm. 274, de 15 de noviembre de 1991); http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/1836
[37] Sentencia 57/1994, de 28 de febrero (BOE núm. 71, de 24 de marzo de 1994) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2574
[38] Sentencia 143/1994, de 9 de mayo (BOE núm. 140, de 13 de junio de 1994) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2660
[39] Sentencia 207/1996, de 16 de diciembre (BOE núm. 19, de 22 de enero de 1997) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/3259
[40] Sentencia 156/2001, de 2 de julio (BOE núm. 178, de 26 de julio de 2001) http://hj.tribunalconstitucional.es/es/Resolucion/Show/4452
[41] Sentencia 127/2003, de 30 de junio (BOE núm. 181, de 30 de julio de 2003) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4902
[42] Sentencia 196/2004, de 15 de noviembre (BOE núm. 306, de 21 de diciembre de 2004); http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/5201
[43] Sentencia 81/2001, de 26 de marzo (BOE núm. 104, de 01 de mayo de 2001) http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4377
[44] Sentencia 156/2001, de 2 de julio; (BOE núm. 178, de 26 de julio de 2001) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4452
[45] Sentencia 83/2002, de 22 de abril; (BOE núm. 122, de 22 de mayo de 2002) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4619

(Sentencia del Tribunal Constitucional 83/2002, de 22 de abril[46], que citan otras muchas anteriores).

El desarrollo de la protección de estos tres derechos se efectúa a través de la L.O. 1/1982, de 5 de mayo, *de protección civil del derecho al honor, la intimidad y la propia imagen*[47]. Los mismos tienen su amenaza más cercana en el ejercicio de las libertades de expresión e información consagradas en el art. 20 CE, siendo preciso ponderar unos derechos frente a los otros, habiéndose consolidado por una abundante doctrina y jurisprudencia los requisitos que deben cumplirse en el ejercicio de la libertad de información y expresión para poderlas considerar constitucionalmente legítimas y hacer prevalecer esos derechos sobre aquéllos del art. 18 CE, a saber, que la información difundida tenga relevancia pública y sea veraz, además de que la manifestación de la información se haga de forma correcta, empleando "expresiones y conceptos correctos, los que resulten necesarios para exponer las ideas", según exige nuestro Tribunal Constitucional desde la Sentencia del asunto *Crespo Martínez*, de 21 de enero de 1988[48].

Los tres derechos que analizamos (honor, intimidad personal y familiar y propia imagen), podrán verse afectados independientemente o de forma conjunta, considerando su proximidad.

La inviolabilidad del domicilio se vincula al derecho a la intimidad de las personas, y protege el ámbito donde la persona desarrolla su vida al amparo de miradas indiscretas. Para el Tribunal Constitucional, el término domicilio es el espacio donde el individuo vive ejerciendo su libertad más íntima, incluyéndose en ese concepto las segundas viviendas, las habitaciones de hotel e incluso los vehículos. La vulneración de ese derecho puede admitirse tanto si la intromisión se produce físicamente como

[46] Citada.
[47] «BOE» núm. 115, de 14/05/1982; https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196
[48] Sentencia 6/1988, de 21 de enero (BOE núm. 31, de 5 de febrero de 1988) http://hj.tribunalconstitucional.es/en/Resolucion/Show/947

si la misma se lleva a cabo mediante aparatos visuales o auditivos. La Constitución señala expresamente que se admite la entrada y registro domiciliarios en caso de "flagrante delito".

La protección del derecho de las comunicaciones como garantía de libertad individual e instrumento de desarrollo cultural, científico y tecnológico colectivo tiene una entidad propia, ya que las comunicaciones deberán resultar protegidas con independencia de su contenido (sean o no íntimas). En el término "comunicaciones" se engloban las postales, telegráficas y telefónicas, debiendo entenderse también comprendidos el correo electrónico, chats u otros medios.

La mayor incidencia de ese derecho está en las comunicaciones telefónicas, planteándose distintos grados de posible vulneración del secreto: intervención, grabación o recuento (STC 217/1989, de 21 de diciembre[49]).

En España se permitirán las intervenciones telefónicas para los delitos graves, entendidos como "delitos calificables de infracciones punibles graves" a lo que el Tribunal Constitucional considera necesario añadir "el bien jurídico protegido y la relevancia social de la actividad" (SSTC 202/2001, de 21 de noviembre[50], y 14/2001, de 29 de enero[51]), tales como el tráfico de drogas a gran escala o delitos contra la salud pública (entre otras, SSTC 32/1994, de 31 de enero[52]; 207/1996, de 16 de diciembre[53]) o también "el uso de tecnologías de la información" (STC 104/2006, de 3 de abril[54]).

[49] Sentencia 217/1989, de 21 de diciembre (BOE núm. 10, de 11 de enero de 1990)
http://hj.tribunalconstitucional.es/es/Resolucion/Show/1423
[50] Sentencia 202/2001, de 15 de octubre (BOE núm. 279, de 21 de noviembre de 2001)
http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4498
[51] Sentencia 14/2001, de 29 de enero (BOE núm. 52, de 01 de marzo de 2001)
http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4310
[52] Sentencia 32/1994, de 31 de enero (BOE núm. 52, de 02 de marzo de 1994)
http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2549
[53] Citada.
[54] Sentencia 104/2006, de 3 de abril (BOE núm. 110, de 09 de mayo de 2006)
https://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/5706

Finalmente, el derecho a la protección de datos de carácter personal (18.4 CE) es un derecho fundamental a través del cual se garantiza a la persona el control sobre sus datos, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. Se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquél que justificó su obtención y se intenta lograr la adecuación y exactitud de las bases de datos, así como su cancelación cuando dejen de ser necesarios, así como el conocimiento y la posibilidad de acceso por parte de los afectados, con un especial deber de protección para los datos denominados sensibles, aquellos que afectan a la ideología, religión, creencias, así como los relativos a la salud (Art. 16.2 CE).

1.6. El derecho fundamental a la intimidad en la jurisprudencia constitucional

Con base en las disposiciones del art. 18 CE y de la LO 1/1982 y la interpretación que nuestra jurisprudencia ha hecho de esos preceptos, obras divulgativas[55] definen el "derecho a la intimidad" como "el derecho a disfrutar de un ámbito propio y reservado para desarrollar una vida personal y familiar plena y libre, excluido tanto del conocimiento como de las intromisiones de terceros"[56].

Nuestro Tribunal Constitucional ha perfilado ese concepto en su jurisprudencia, estableciendo, como recoge la definición del DEJ que venimos de reproducir, que el derecho a la intimidad tiene por objeto garantizar al individuo un ámbito reservado de su vida, excluido tanto del conocimiento como de las intromisiones de terceros

[55] MUÑOZ MACHADO, S. (director): Diccionario del Español Jurídico elaborada por la Real Academia de la Lengua Española junto con el Consejo General del Poder Judicial. Espasa. Madrid, 2016.
[56] Veremos seguidamente como esa definición coincide con la establecida jurisprudencialmente por el TC en sus Sentencias 134/1999 y 144/1999.

(STC 144/1999 de 22 de julio[57]). Ese derecho implica, pues, la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, ámbito necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana[58].

La STC 134/1999 de 15 de julio[59] establece que "el derecho a la intimidad salvaguardado en el art. 18.1 C.E. tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad (SSTC 73/1982[60], 110/1984[61], 107/1987[62], 231/1988[63], 197/1991[64], 143/1994[65] y 151/1997[66]). El derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida. El art. 18.1 C.E. no garantiza una intimidad determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona

[57] Citada. Sentencia 144/1999, de 22 de julio (BOE núm. 204, de 22 de agosto de 1999) http://hj.tribunalconstitucional.es/HJ/es-ES/Resolucion/Show/SENTENCIA/1999/144
[58] CASTÁN TOBEÑAS, J., «Los derechos de la personalidad», *Revista General de Legislación y Jurisprudencia*, julio-agosto 1952, págs. 5-62.
[59] Sentencia 134/1999, de 15 de julio; (BOE núm. 197, de 18 de agosto de 1999) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/3876
[60] Sentencia 73/1982, de 2 de diciembre (BOE núm. 312, de 29 de diciembre de 1982) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/115
[61] Sentencia 110/1984, de 26 de noviembre (BOE núm. 305, de 21 de diciembre de 1984) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/363
[62] Sentencia 107/1987, de 25 de junio (BOE núm. 163, de 09 de julio de 1987) http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/839
[63] Citada.
[64] Citada.
[65] Citada.
[66] Sentencia 151/1997, de 29 de septiembre (BOE núm. 260, de 30 de octubre de 1997); http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/3416

reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio. Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida, lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos".

Toda persona tiene, por tanto, "derecho a un espacio resguardado de la curiosidad ajena, sea cual sea el contenido de ese espacio", y aunque, según nuestro Tribunal Constitucional "la personalidad pública debe optar por un cierto riesgo en la lesión de sus derechos de la personalidad" (STC número 165/1987[67]), "el riesgo asumido por el personaje con notoriedad pública no implica aminoración de su derecho a la intimidad o al honor o a la propia imagen, cuya extensión y eficacia sigue siendo la misma que la de cualquier otro individuo" (STC 134/1999 de 15 de julio[68])". En todo caso, según esa misma sentencia "no pueden imponer el silencio a quienes únicamente divulgan, comentan o critican lo que ellos mismos han revelado (...)".

1.7. Los nuevos retos jurídicos del derecho fundamental a la intimidad

Señalaban los autores WARREN Y BRANDEIS en el artículo mencionado y analizado en el presente Capítulo como resulta preciso que el derecho se adapte y evolucione para dar respuesta a los nuevos retos que plantea la evolución tecnológica y que es preciso regular adecuadamente para permitir la convivencia en sociedad.

[67] Sentencia 165/1987, de 27 de octubre (BOE núm. 279, de 21 de noviembre de 1987); http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/897
[68] Citada.

Y es que, es una evidencia que los derechos fundamentales han ido evolucionando junto con el ser humano, modificándose y adaptándose a las distintas circunstancias de la sociedad. Es un reflejo del aforismo romano "ubi societas, ibi ius", o "donde hay sociedad, hay derecho", y que expresa precisamente esa capacidad de adaptación del derecho para dar respuesta a los nuevos retos que se plantean en la sociedad según ésta va cambiando.

Hemos hablado en el primer epígrafe del presente Capítulo 1 de los derechos fundamentales de primera, segunda y tercera generación, siendo preciso ahora aludir a aquella otra generación de derechos (la cuarta), a través de la cual se da respuesta a las nuevas necesidades a las que el hombre debe enfrentarse como consecuencia de la revolución tecnológica en la que nos encontramos inmersos.

Esa revolución tecnológica implica la creación de infinidad de herramientas y aparatos que han alterado de manera significativa las relaciones del hombre en sociedad. La denominada *Sociedad de la Información* ha determinado la creación de esa nueva generación de derechos relacionados directamente con las nuevas tecnologías de la información y la comunicación (TICs)[69], en la que las libertades y derechos se han introducido en el espacio digital, constituyendo un nuevo reto para el sistema jurídico lograr su reconocimiento y protección por parte del Estado.

En esa cuarta generación de derechos se enmarca el derecho a la autodeterminación informativa, sobre el que volveremos en el Capítulo 3 del presente trabajo, y que constituye la evolución de una línea jurisprudencial que parte del derecho a la intimidad personal y familiar, pasa por el derecho a la autodeterminación informativa, y evoluciona hasta la protección de datos de carácter personal, entroncando con el

[69] Son ejemplos: el derecho de acceso a la informática; el derecho al uso del espectro radioeléctrico y de las infraestructuras para los servicios en línea, el derecho a la autodeterminación informativa o la seguridad digital.

apartado cuarto del art. 18 CE y el segundo del artículo 10 CE, y finalizando con la formulación del derecho al olvido digital como nuevo derecho fundamental.

El derecho a la protección de datos de carácter personal se reconoce como un "verdadero derecho fundamental autónomo e independiente del derecho a la intimidad"[70], que nuestro TC define como "poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[71].

Es claro que el concepto de intimidad es heterogéneo y dinámico, por lo que su protección debe poder adaptarse al contexto y a los cambios tecnológicos, siendo preciso encontrar el equilibrio adecuado entre su protección y la protección de otros derechos y valores que pudieran estar en juego (seguridad, competencia, innovación, etc.)

1.7.1. Internet y derecho a la intimidad

Ya hemos dicho que la evolución y los avances tecnológicos plantean nuevos retos para la intimidad, y que la creación de Internet a finales de los años sesenta, primero como una red de defensa militar (ARPANET)[72], y posteriormente como una red de comunicación que ha cambiado nuestra forma de socializar, adquirir productos y/o servicios y relacionarnos[73].

[70] PIÑAR MAÑAS, J.L: "Protección de datos: origen, situación actual, y retos de futuro", en *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.
[71] STC 292/2000, de 30 de noviembre.
[72] BARRIO ANDRÉS, M.: *Fundamentos del derecho de Internet*. Ed. Centro de Estudios Políticos y Constitucionales, Madrid 2017.
[73] MUÑOZ MACHADO, S.: *La regulación de la Red. Poder y Derecho en Internet,* Ed. Taurus, 2000.

La propia Internet ha sufrido una evolución impresionante desde el momento de su creación. En un primer momento, la denominada Web 1.0 permitía fundamentalmente la búsqueda de información por parte del usuario. De ese primer concepto más "estático", se fue pasando de forma progresiva a una segunda versión más evolucionada (Web 2.0), en la que el usuario podía interactuar y participar en la web como "creador de contenidos", revistiéndola de un carácter más "social", siendo ejemplos de esta segunda etapa de Internet la creación de redes sociales, blogs o wikis. Finalmente, una tercera (pero no última) etapa, la Web 3.0, que surge en el Internet de las cosas (neveras que avisan de que es preciso reponer determinados productos, luces que se encienden o apagan siguiendo determinadas consignas, coches sin conductor…), y aplicaciones que pueden interactuar e interconectarse entre sí. Se habla en la actualidad de una cuarta etapa de Internet (Web 4.0), que es la web predictiva, que permite dar soluciones concretas a las necesidades de los usuarios[74].

1.7.2. Tratamiento de datos e intimidad

Pero no es solo Internet la que plantea retos al derecho. También plantean interesantes problemas jurídicos en los que puede estar implicado el derecho fundamental a la intimidad otras invenciones como los drones, la posibilidad de geolocalizar a las personas a través de sus smartphones, los escáneres que permiten tomar imágenes de cuerpo entero, las tecnologías de reconocimiento facial y de voz, los que posibilitan el rastreo de la actividad en Internet (páginas web visitadas, actividad en redes sociales; historial de compras online; etc.).

Para el desarrollo de todas esas nuevas tecnologías y su funcionamiento, es de singular importancia la toma de datos y de su tratamiento, motivo por el que es preciso contar

[74] TOURIÑO, A.: *El derecho al olvido y a la intimidad en Internet,* Ed. Catarata, Madrid, 2014.

con una legislación en materia de protección de datos que permita garantizar al individuo el respeto de sus derechos. Más aún cuando se ha revelado, de forma reciente, el uso que algunos Gobiernos[75] o algunas compañías[76] hacen de esos datos personales, hechos que han motivado exigencias de transparencia y seguridad por parte de los ciudadanos, sus titulares.

Tanto la legislación europea como la española en materia de protección de datos han sido y son unas de las más punteras de todo el mundo, desde el inicio de su reconocimiento positivo en los ordenamientos de los distintos estados miembros de la Unión Europea y el propio comunitario a partir de la segunda mitad de los años 60 y hasta la reciente entrada en vigor del Reglamento General de protección de datos en el mes de mayo de 2018 pasado, instaurando restricciones e imponiendo obligaciones a los responsables del tratamiento en beneficio del titular de los derechos, consolidándose como una de las normativas más modernas en la materia de todo el planeta. Abordaremos ese desarrollo en los Capítulos 2 y 3 de la presente tesis, motivo por el que no nos detendremos mucho más en esos extremos en el presente apartado, con el fin de evitar ser reiterativos.

En el aludido contexto ha encontrado también su reconocimiento normativo el derecho al olvido digital, conceptuado como el derecho del interesado a la supresión, por parte del responsable del tratamiento, de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando ya no sean necesarios para los fines para los que fueron tomados, cuando el interesado revoque su consentimiento, se oponga al tratamiento o los datos fueran recabados de

[75] Las revelaciones sobre el espionaje masivo de la Agencia Nacional de Seguridad de EE UU, hechas por el exempleado de la CIA EDWARD SNOWDEN, tuvieron gran impacto en la opinión pública internacional.
https://www.20minutos.es/noticia/1850380/0/caso-snowden/cronologia/espionaje-ee-uu/#xtor=AD-15&xts=467263

[76] Aludimos al denominado "escándalo de Cambridge Analitics", empresa que se vio involucrada, en marzo de 2018, en un escándalo después de que un exempleado revelara algunas prácticas de la compañía para influir en elecciones políticas, en el que se vio también comprometida la credibilidad de Facebook.

forma ilícita, entre otras circunstancias[77]. Derecho sobre el que más adelante volveremos con mayor detenimiento y que constituye la materia fundamental del presente trabajo.

1.7.3. Economía de datos e intimidad

Ya hemos dicho que son muchos los nuevos retos jurídicos a los que tiene que enfrentarse el tradicional derecho a la intimidad como consecuencia de los avances tecnológicos, sin que puedan olvidarse, en todo caso, aquéllos derivados del interés comercial y del propio valor económico que tienen los datos.

La Comisión Europea estima que el valor de la economía de los datos en la UE ascendía a 257 000 millones EUR en 2014, lo que equivale al 1,85 % del PIB de la UE. La cifra aumentó hasta los 272 000 millones EUR en 2015, equivalente al 1,87 % del PIB de la UE (crecimiento interanual del 5,6 %). La misma estimación prevé que, si se implantan a tiempo las condiciones marco políticas y jurídicas para la economía de los datos, su valor se situará en los 643 000 millones EUR para 2020, lo que representaría el 3,17 % del PIB total de la UE[78].

Los datos tienen mucho valor, por ejemplo, para el sector publicitario, ya que permiten desarrollar "publicidad personalizada", teóricamente menos agresiva y menos molesta que la publicidad de productos que son ajenos al interés del consumidor, y que permitirá recibir información fundamentalmente de aquellos productos que se quieren o desean. No obstante, también entraña riesgos,

[77] La definición está tomada del art. 17 del RGPD.
[78] Comunicación de la Comisión al Parlamento Europeo y al Consejo, al Comité económico y social europeo y al Comité de las regiones "La Construcción de una Economía de los datos europea". 10.1.2017
http://ec.europa.eu/transparency/regdoc/rep/1/2017/ES/COM-2017-9-F1-ES-MAIN-PART-1.PDF

fundamentalmente vinculados a la pérdida progresiva de intimidad, así como la eventual posibilidad de que el vendedor detecte las condiciones del comprador y pueda ofertarle los mismos productos a un precio "adaptado" y eventualmente menos conveniente que el que pudiera ofrecerse a otro consumidor menos desahogado económicamente.

Esa recopilación, tratamiento y comercialización de nuestros datos no solo constituye un potencial daño a nuestra intimidad, sino también un potencial daño económico, considerando que el uso imprevisible de nuestros datos puede no suponer un coste para su titular, pero si la constatación de que terceros puedan lucrarse con el uso de nuestros datos, lo cual no dejaría de ser igualmente injusto.

1.7.4. Redes sociales: de la intimidad a la "extimidad"

Internet no es solo una red informática mundial. También es una comunidad de usuarios que crece exponencialmente. Según la AEPD las redes sociales son "servicios prestados a través de Internet que permiten a los usuarios crear un perfil público en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines, o no, al perfil publicado"[79].

El Prof. MORENO NAVARRETE[80] distingue, por sus fines, tres tipos de redes sociales: las generalistas, las corporativas o profesionales y las educacionales. A su vez, entre las generalistas incluye, de una parte, las plataformas de intercambio de contenidos,

[79] Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, AEPD y Instituto Nacional de Tecnologías de la Comunicación https://www.uv.es/limprot/boletin9/inteco.pdf

[80] MORENO NAVARRETE, M.A.: "Aspectos jurídicos privados de las tecnologías Web 2.0" en BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador): *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

como sería por ejemplo Youtube; de otra parte, las redes sociales basadas en información de perfil, que son las más utilizadas y de las que es ejemplo Facebook; y finalmente las redes de microblogging como es Twittter. El ejemplo paradigmático de red social profesional es LinkedIn.

En nuestro país, casi trece millones de personas forman parte de alguna red social. Redes que tienen un crecimiento exponencial del 20% anual.

La presencia del individuo en redes sociales tiene una importantísima transcendencia económica, considerando que los datos que la persona introduce en esa red social al abrir su perfil y alimentarlo diariamente, permite crear auténticos perfiles de sus gustos y preferencias. Los gestores de esas redes sociales aprovechan esa información facilitada a través del servicio que se presta al usuario "gratuitamente" para segmentar el público al que puede dirigirse, por ejemplo, la publicidad, que con toda evidencia será así más efectiva, al menos teóricamente.

También es evaluable económicamente para las marcas esa presencia en redes sociales (en términos del número de seguidores que puedan tener los usuarios), que miden esa "influencia" y remuneran a esas concretas personas en dinero o en especie por mostrar sus productos, dependiendo el precio precisamente de la presencia en unas y otras redes sociales, y en detrimento, generalmente, de su privacidad.

Pero al margen de la relevancia económica de esa presencia en redes sociales, sea para las personas presentes en las mismas, sea para los gestores de esas redes sociales, es preciso incidir, a los efectos del presente trabajo, en que a diferencia de cuanto sucedía en otros momentos de la Historia, hoy somos nosotros mismos quienes, con nuestra forma de vida y nuestra actuación personal, exponemos en muchas ocasiones nuestra intimidad a través de esas redes sociales, en actuaciones que pueden erosionar gravemente nuestro derecho fundamental a la intimidad, si no llegando al extremo de profesionalizar esa presencia como hacen los "influencers", si compartiendo con

terceros situaciones cotidianas que forman parte de ese reducto considerado como íntimo y que antes se prefería mantener reservado para uno mismo.

Hay autores que han denominado ese fenómeno con el término "extimidad"[81], que designa toda esa exposición voluntaria (exhibicionista, incluso), fundamentalmente a través de las redes sociales.

Algunos autores[82] han señalado como, "la raíz interiorista del derecho a la intimidad, tal y como se ha concebido hasta ahora, ha cambiado hacia un concepto externo de lo íntimo para configurar una personalidad que nos defina y distinga frente a los demás como medio de ser reconocidos y estimados en ese entorno virtual, mediante un debilitamiento de lo introspectivo en favor de la externalización de nuestra personalidad"[83].

Concluyendo que Internet, las redes sociales y las comunidades virtuales "debilitan el concepto de intimidad", "exponiendo información e imágenes de su vida personal de forma voluntaria". Esta práctica produciría una "redefinición del concepto de intimidad", y de los eventuales quebrantos de ésta. Porque como ya hemos dicho, las normas y la jurisprudencia han estimado que en la ponderación que ha de hacerse entre los derechos en conflicto (libertad de información/expresión vs. intimidad) debe considerarse el ámbito de reserva que las personas "han mantenido para si mismos o su familia", que pudiera no ser el caso si su presencia es muy activa en una o varias redes sociales. Por ello, es fundamental la educación y la concienciación, sobre todo de los más jóvenes, respecto de la necesidad de hacer un uso prudente de las

[81] El primero en acuñar el concepto fue el psicoanalista Jacques Lacan, quien lo planteó como una paradoja: lo éxtimo es aquello que está más cerca del interior, pero sin dejar de encontrarse en el exterior.
[82] OROZCO PARDO con cita a PAULA SIBILA en "Intimidad, privacidad, "extimidad" y protección de datos del menor. ¿Un cambio de paradigma", en BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador): *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.
[83] SIBILA, P.: *La intimidad como espectáculo*. Ed. Fondo de cultura económica de Argentina, S.A., Buenos Aires, 2008.

redes sociales, la importancia de no compartir datos ni imágenes comprometidas o que les puedan comprometer en el futuro, vigilando desde jóvenes su propia reputación online, y evitando aquellas situaciones que en un futuro puedan ponerles en situación vulnerable como consecuencia de contenidos compartidos por iniciativa propia en la época de juventud.

Pero a pesar de todos los interesantes retos, no solo jurídicos (también éticos, económicos, etc.), que las realidades tecnológicas e Internet plantean, no dejan de ser también excelentes herramientas y aliados para el progreso, con infinitas posibilidades para la ciencia, la comunicación, la educación, o la cultura. Herramientas que bien empleadas constituyen un innegable avance y una revolución equivalente a las industriales que tuvieron lugar en los siglos XVIII y XX, como así la bautizó el propio Parlamento Europeo en 2006[84].

[84] RIFKIN, J.: "The Third Industrial Revolution: How the Internet, Green Electricity, and 3-D Printing are Ushering in a Sustainable Era of Distributed Capitalism" https://web.archive.org/web/20120331180815/http://www.worldfinancialreview.com/?p=1547

CAPÍTULO 2

LA GESTACIÓN DEL DERECHO AL OLVIDO DIGITAL

EN LA LEGISLACIÓN COMUNITARIA EUROPEA Y EN LA ESPAÑOLA.

SUMARIO: 2.1. UN PRIMER ANTECEDENTE: EL CONVENIO 108 DEL CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LAS PERSONAS RESPECTO DEL TRATAMIENTO AUTOMATIZADO DE SUS DATOS FIRMADO EN 1981; 2.2. EL ART. 286 DEL TCE (AHORA, ART. 16.1 TFUE); 2.3 LA DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 24 DE OCTUBRE DE 1995, RELATIVA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS; 2.4 EL PRINCIPIO DE CALIDAD DE LOS DATOS Y LOS DERECHOS DE OPOSICIÓN Y CANCELACIÓN COMO ANTECEDENTES FUNDAMENTALES DEL DERECHO AL OLVIDO DIGITAL; 2.5 EL ART. 8 DE LA CARTA DE DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA; 2.6. EL RECONOCIMIENTO EN ESPAÑA DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA COMO ANTECEDENTE NECESARIO AL DEL DERECHO FUNDAMENTAL AL OLVIDO DIGITAL; 2.7. MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS EN ESPAÑA; 2.7.1 LORTAD; 2.7.2 LOPD; 2.7.3 REGLAMENTO DE DESARROLLO DE LA LOPD; 2.7.4 NORMATIVA AUTONÓMICA DE PROTECCIÓN DE DATOS; A.) MADRID; B.) CATALUÑA; C.) PAÍS VASCO; D.) ANDALUCÍA; 2.7.5 LEYES SECTORIALES CON INCIDENCIA SOBRE LA PROTECCIÓN DE DATOS.

2.1. Un primer antecedente: el Convenio 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de sus datos firmado en 1981

A pesar de que el derecho al olvido digital se ha reconocido de forma expresa en la legislación comunitaria europea de forma reciente, son varios los antecedentes que han precedido a ese reconocimiento positivo y que nos permiten rastrear el germen de ese nuevo derecho.

El mismo hay que buscarlo en los principios generales, determinantes del libre desarrollo de la personalidad del individuo, y en el derecho a la protección de datos de carácter personal, al que está íntimamente ligado.

La primera vez que estas preocupaciones tuvieron reflejo en la escena supranacional y, por tanto, el primer texto en el que podemos encontrar un antecedente de este derecho es el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[85], firmado en Estrasburgo el 28 de enero de 1981 y ratificado por España el 27 de enero de 1984, que entró en vigor el 1 de octubre de 1985[86].

Los países firmantes de ese Convenio fueron Suecia[87], Francia[88], España[89]; Noruega[90] y la República Federal de Alemania[91], y su objeto, según dispone textualmente su preámbulo era "llevar a cabo una unión más íntima entre sus miembros", "basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales", "considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados". "Reafirmando al mismo tiempo su compromiso en favor de la libertad de información sin tener en cuenta las fronteras" y "reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos".

El convenio está actualmente en vigor en 53 países, y consta de veintisiete artículos divididos en siete capítulos. Reconoce en su artículo quinto y por primera vez en un texto legal, el "derecho a la calidad de los datos", disponiendo que en virtud de ese

[85] http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DCONVENIO%2520108.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1202800216772&ssbinary=true
[86] BOE núm. 274 de 15-11-1985
[87] 29-9-1982
[88] 24-3-1983;
[89] 31-1-1984
[90] 20-2-1984
[91] 19-6-1985

principio los Estados firmantes del Convenio se comprometen a que los datos personales tratados se obtengan y traten legítimamente; sean registrados para finalidades determinadas y legítimas y no se empleen de forma incompatible con dichas finalidades; sean adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales hayan sido registrados; sean exactos y, en su caso, puestos al día; y se conserven solo durante el tiempo necesario para esas finalidades para las cuales se hubieran registrado.

Ese texto normativo constituye, según SIMÓN CASTELLANO[92], un "primer instrumento jurídico internacional con vocación universal para la protección de los datos de carácter personal", estableciendo a su vez un antecedente relevante y claro para la Directiva 95/46/CE, y en consecuencia para todo el cuerpo normativo de la protección de datos en el marco de los Estados miembros de la Unión Europea.

El Convenio n.º 108 del Consejo de Europa es, a día de la fecha, el único instrumento multilateral jurídicamente vinculante en el ámbito de la protección de los datos de carácter personal, y acaba de modernizarse para adaptarse a las novedades legislativas en materia de protección de datos.

Recientemente se ha rubricado una versión actualizada del Convenio (denominado "Convenio nº 108 +"), con el fin de que refleje los mismos principios que los recogidos en las nuevas normas sobre protección de datos de la UE, ayudando a establecer un conjunto uniforme de reglas de alto nivel para la protección de datos[93].

La firma de ese protocolo revisado[94] tuvo lugar el diez de octubre de 2018 pasado y contó con el apoyo en su estreno de un total de veinte países de la organización

[92] SIMÓN CASTELLANO, P.: *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia TJUE de mayo de 2014*. 1ª Edición. Ed. Bosch, Barcelona 2015, pág. 189.
[93] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
[94] Incluimos un cuadro comparativo de ambas versiones del Convenio 108 como Anexo II
Fuente: https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958

paneuropea, entre ellos España, Alemania, Francia, Reino Unido, Rusia y Portugal, además de Uruguay[95].

La Comisión Europea animará asimismo a los países no pertenecientes a la Unión a ratificar tanto ese "Convenio n.º 108 +" del Consejo de Europa, como su Protocolo Adicional[96]. Según publicó LA VANGUARDIA[97] ese día, "Argentina, Chile y Costa Rica podrían ser los próximos países en adherirse al Convenio, mientras que Brasil acaba de solicitarlo".

2.2 El art. 286 TCE

El art. 286 TCE, en vigor desde el 12 de junio de 1985 y hasta el 1 de diciembre de 2009, e incorporado posteriormente al TFUE (ahora art. 16.1 TFUE[98]), reconoce el derecho de toda persona "a la protección de los datos personales que le conciernen", encomendando al Parlamento y al Consejo de la UE la aprobación de las normas que pudieran ser necesarias para la protección de las personas físicas respecto del tratamiento de sus datos de carácter personal. En ese contexto, el legislador comunitario ha aprobado los textos normativos que seguidamente se dirán.

---

[95] EFE.- "España y 20 países firman protocolo para el Convenio de Protección de Datos". https://www.lavanguardia.com/politica/20181010/452291023498/espana-y-20-paises-firman-protocolo-para-el-convenio-de-proteccion-de-datos.html

[96] Así se recoge también en la Comunicación de la Comisión al Parlamento Europeo y al Consejo "Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento General de protección de datos a partir del 25 de mayo de 2018" https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN

[97] Citada en 95.

[98]

> *1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
> *2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.*
> *Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea*

2.3. La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

La Directiva 95/46/CE[99] supuso un hito en la regulación de la protección de datos de carácter personal. Realizamos seguidamente un breve análisis del contenido y alcance de sus disposiciones[100].

Ese texto normativo se aprobó el 13 de diciembre de 1995 y fue publicada en el DO L 281 de 23 de noviembre de 1995, con plazo de trasposición a los Estados miembros de 24 de octubre de 1998. Ha estado vigente desde ese momento y hasta la entrada en vigor del RGPD, el día 25 de mayo de 2018.

La Directiva creó un marco regulador con el objeto de establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. Con ese fin, la Directiva establece límites a la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales[101].

Respecto del ámbito de aplicación de esa Directiva (derogada con la entrada en vigor del RGPD), la misma se aplicaba "a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en

[99] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31995L0046
[100] GARRIGA DOMÍNGUEZ, A.: *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la Computación Ubicua*. Ed. Dykinson, S.L. Madrid, 2015.
[101] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012

él"[102]. No se aplicaba, en cambio, "ni al tratamiento efectuado por una persona física en ejercicio de actividades exclusivamente privadas o domésticas"; o "al ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado"[103].

Su objetivo era "garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (artículo 1º)", "estableciendo los criterios fundamentales para que el tratamiento sea lícito y los principios relativos a la calidad de los datos".

Para que el tratamiento de los datos de carácter personal pueda reputarse lícito (art. 7), según los estándares de la Directiva, deben cumplirse los siguientes requisitos:

- el interesado ha dado inequívocamente su consentimiento; o
- el tratamiento es necesario para el cumplimiento de un contrato en el que sea parte el interesado; o
- el tratamiento es necesario para el cumplimiento de una obligación legal del responsable del tratamiento; o
- el tratamiento es necesario para proteger los intereses vitales de la persona de cuyos datos se trate; o
- el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero, o
- el tratamiento es necesario para los fines de interés legítimo del responsable del tratamiento o de un tercero, siempre que sobre dichos intereses no

[102] Apartado 1º art. 3º
[103] Apartado 2º art. 3º.

> prevalezcan los intereses del interesado en el ámbito de los derechos y libertades que requieren protección.

Respecto del principio de calidad de los datos (artículo 6), que es un antecedente clave del posteriormente reconocido derecho al olvido digital, dispone que debe aplicarse a todas las actividades de tratamiento de datos lícitas, debiendo aplicarse los siguientes principios: los datos personales tratados debían serlo de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, ser adecuados, pertinentes y no excesivos, exactos y, cuando sea necesario, actualizados, y debiendo conservarse durante un período no superior al necesario y solo para los fines para los que fueron recogidos. Es patente que el contenido del art. 6 de la Directiva es muy similar al del Convenio 108 al que nos hemos referido en el apartado 2.1 del presente Capítulo.

Además, la Directiva recoge en su Sección III lo que denomina "categorías especiales de tratamiento". En particular, dispone que "deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico" (artículo 8).

Respecto de las personas cuyos datos son tratados (los interesados), se les reconoce expresamente la posibilidad de ejercer los derechos siguientes:

- El derecho a obtener información: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) (artículo 10).

- El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener copia de sus propios datos del responsable del tratamiento (artículo 12).

- El derecho a oponerse al tratamiento de los datos: el interesado deberá tener el derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación (artículo 14).

Otros aspectos relevantes del tratamiento de datos son los que siguen:

- **Las excepciones y limitaciones a los derechos del interesado (artículo 13):** se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

- **La confidencialidad y la seguridad del tratamiento (artículos 16 y 17):** las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

- **La notificación del tratamiento a la autoridad de control (artículo 18):** el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Disponía la Directiva que las legislaciones nacionales debían prever un recurso judicial (artículo 22) para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufrieran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrían derecho a obtener la reparación del perjuicio sufrido (artículo 23).

Se autorizaba la transferencia de datos personales (Capítulo IV, artículos 25 y 26) de un Estado miembro a un tercer país, siempre y cuando este último garantizase un nivel de protección adecuado; por el contrario, si bien no se autorizaba la transferencia cuando no se garantizaba un nivel adecuado de protección, esta norma general tenía varias excepciones enumeradas en la Directiva; p. ej. cuando el propio interesado consentía la transferencia, en el caso de la celebración de un contrato, cuando sea necesario por motivos de interés público y también si el Estado miembro había autorizado normas empresariales vinculantes o cláusulas contractuales.

La Directiva pretendía facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyeran a una correcta aplicación de las disposiciones nacionales y comunitarias (artículo 27).

Cada Estado miembro debía designar una o varias autoridades públicas, independientes, encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de esa Directiva (artículo 28).

Se creaba, finalmente, un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales (artículo 29), que estaba compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión. Grupo de trabajo que se ha conocido desde el momento de su creación con el sobrenombre "Grupo de trabajo del artículo 29".

2.4. El principio de "calidad de los datos" y los derechos de oposición y cancelación como antecedentes fundamentales del derecho al olvido digital

Como se acaba de exponer en el apartado precedente, la recogida y el tratamiento automatizado de datos de carácter personal, para que sea lícito, debe hacerse conforme a los principios de adecuación, pertinencia, proporcionalidad y exactitud que integran el principio denominado como de "calidad de los datos".

Esos principios están recogidos tanto en el artículo 6 de la Directiva que venimos de analizar en el apartado anterior como, a nivel nacional, en el art. 4 de la LOPDDD. Los datos personales objeto de tratamiento automatizado han de ser exactos (artículos 6.1.e) de la Directiva y 4.1 LOPDDD), adecuados, pertinentes y no excesivos en

relación con el ámbito y las finalidades para las que se hayan obtenido (artículos 6.1.d de la Directiva y arts. 93 y 94 de la LODPDD que recogen expresamente el derecho a que los datos impertinentes o excesivos sean retirados).

La mayoría de la doctrina ha visto en esos principios y derechos el antecedente directo del nuevo derecho al olvido digital, al entender que este último impone al responsable del tratamiento la obligación de suprimir los datos de carácter personal precisamente cuando éstos han dejado de ser exactos, adecuados o resultan excesivos, en relación con los fines para los que fueron recogidos.

El derecho al olvido digital refuerza, al fin y al cabo, los principios de finalidad, calidad y minimización de los datos, atendiendo a una demanda nueva y a una realidad distinta de aquélla en la que se publicó la Directiva 95/46, derogada tras la entrada en vigor del reciente RGPD.

2.5. El art. 8 de la Carta de derechos fundamentales de la Unión Europea

Con posterioridad a la aprobación y trasposición de la Directiva 95/46 en los distintos Estados miembros de la Unión Europea, constituye también un antecedente de referencia (a pesar de que en aquel momento temporal el pensamiento de los legisladores europeos estuviera aún alejado de un reconocimiento normativo del derecho al olvido digital), el hecho de que con la adopción del Tratado de Lisboa, en el año 2007[104], se reconociese valor jurídico a la Carta de derechos fundamentales de

[104] Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (DO C 306 de 17.12.2007), ratificado por España el veintiséis de septiembre de dos mil ocho https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18898

la Unión Europea[105], cuyo artículo 8[106] reconoció por vez primera y con carácter de derecho fundamental el derecho a la protección de datos de carácter personal.

Ese derecho se incluyó en esa Carta, al entenderse necesario para garantizar la correcta aplicación de los principios de protección de datos al tan cambiante contexto que determinaba la constante evolución de las nuevas tecnologías.

Algunos autores, como RUIZ MIGUEL[107], han sido muy críticos con la conformación del derecho a la protección de datos de carácter personal por la vía de su inclusión en la Carta de derechos fundamentales de la UE, subrayando tanto los problemas normativos que de esa conformación se derivan, así como la "insuficiencia" del contenido de ese derecho y el también problemático desarrollo de su titularidad, límites y garantías.

Por muchas deficiencias técnicas que ese reconocimiento pudiera tener, es innegable que su incorporación a la CDFUE supuso un hito y un avance muy relevante en aquél momento temporal, y "en el proceso de debate público sobre la reforma del derecho europeo de protección de datos" que seguiría a ese reconocimiento, y ello a pesar de que "nada hiciera presagiar que [en el ordenamiento comunitario] fuera a adoptarse previsión expresa alguna referida al derecho al olvido", en palabras de ARTEMI RALLO[108], y como ya hemos apuntado anteriormente.

---

[105] http://www.europarl.europa.eu/charter/pdf/text_es.pdf

[106] *"Artículo 8: Protección de datos de carácter personal:*
1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente."

[107] RUIZ MIGUEL, C.: "El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: análisis crítico". *Revista de Derecho Comunitario Europeo*, año 7, núm. 14, Enero-abril 2003.

[108] RALLO, A.: "El derecho al olvido en Internet. Google vs. España". *Colección "cuadernos y debates",* Centro de Estudios Políticos y Constitucionales, Madrid, 2014. Págs. 34 y ss.

2.6 El reconocimiento en España del derecho a la autodeterminación informativa como antecedente necesario al reconocimiento del derecho fundamental al olvido digital

Así como en el derecho comunitario europeo se iba gestando un derecho a la protección de datos de carácter personal, también en España iba apareciendo y consolidándose ese mismo derecho de forma paralela.

El primer reconocimiento jurisprudencial en España del derecho a la protección de datos de carácter personal como un verdadero derecho independiente y autónomo se produce a través de dos importantísimas Sentencias de nuestro Tribunal Constitucional[109], ambas dictadas el 30 de noviembre del año 2000 con los números 290[110] y 292[111], respectivamente.

La segunda (STC 292/2000), es la que consagró de forma definitiva el reconocimiento del derecho a la protección de datos, como evolución de una línea jurisprudencial que parte del derecho a la intimidad personal y familiar, pasa por el derecho a la autodeterminación informativa, y evoluciona hasta la protección de datos de carácter personal, entroncando con el apartado cuarto del art. 18 CE y el segundo del artículo 10 CE.

De esa resolución judicial destacan, por su transcendencia, los fundamentos de derecho 7º y 8º que reproducimos seguidamente por su claridad e importancia:

---

[109] HERNÁNDEZ LÓPEZ, J.M.: *El Derecho a la Protección de Datos personales en la Doctrina del Tribunal Constitucional*, Ed. Thomson Reuters Aranzadi, Pamplona 2013.
[110] Sentencia 290/2000, de 30 de noviembre; (BOE núm. 4, de 04 de enero de 2001); ECLI:ES:TC:2000:290
http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4274
[111] Sentencia 292/2000, de 30 de noviembre; (BOE núm. 4, de 04 de enero de 2001); ECLI:ES:TC:2000:292
http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4276

"De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

A esas conclusiones fundamentales para la conformación del derecho a la protección de datos como un derecho autónomo[112], se añaden las alcanzadas en el fundamento de derecho siguiente (el octavo), en el que se determina:

[112] VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo: a propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, núm. 41, 1994, págs. 173-187.

"Estas conclusiones sobre el significado y el contenido del derecho a la protección de datos personales se corroboran, atendiendo al mandato del art. 10.2 CE, por lo dispuesto en los instrumentos internacionales que se refieren a dicho derecho fundamental. Como es el caso de la Resolución 45/95 de la Asamblea General de las Naciones Unidas donde se recoge la versión revisada de los Principios Rectores aplicables a los Ficheros Computadorizados de Datos Personales. En el ámbito europeo, del Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal hecho en Estrasburgo el 28 de enero de 1981, del que hemos dicho en la STC 254/1993, FJ 4, que no se limita "a establecer los principios básicos para la protección de los datos tratados automáticamente, especialmente en sus arts. 5, 6, 7 y 11", sino que los completa "con unas garantías para las personas concernidas, que formula detalladamente su art. 8", al que han seguido diversas recomendaciones de la Asamblea del Consejo de Europa.

Por último, otro tanto ocurre en el ámbito comunitario, con la Directiva 95/46, sobre Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y la Libre Circulación de estos datos, así como con la Carta de derechos fundamentales de la Unión Europea del presente año, cuyo art. 8 reconoce este derecho, precisa su contenido y establece la necesidad de una autoridad que vele por su respeto. Pues todos estos textos internacionales coinciden en el establecimiento de un régimen jurídico para la protección de datos personales en el que se regula el ejercicio de este derecho fundamental en cuanto a la recogida de tales datos, la información de los interesados sobre su origen y destino, la facultad de rectificación y cancelación, así como el consentimiento respecto para su uso o cesión. Esto es, como antes se ha visto, un haz de garantías cuyo contenido hace posible el respeto de este derecho fundamental".

Como acertadamente subraya el Prof. PIÑAR MAÑAS[113], la Sentencia del Tribunal Constitucional que venimos de transcribir "reconoce la existencia del Derecho a la protección de datos como un derecho autónomo e independiente del Derecho a la intimidad; determina su contenido esencial; lo relaciona no solo con el artículo 18.4 de la Constitución, sino también con el 10.2" y además, en el Fundamento jurídico 8º cita de forma expresa diversos instrumentos internacionales y en particular […] la Carta europea de derechos fundamentales".

El mismo análisis realiza MURILLO DE LA CUEVA[114] concluyendo que: "el Tribunal Constitucional, en su Sentencia 292/2000, de 30 de noviembre, estableció de forma terminante que se trata de un nuevo derecho fundamental, el derecho a la protección de datos de carácter personal, cuyo propósito no es otro que ofrecer a las personas los medios para controlar el uso ajeno de la información personal que les concierne". "Derecho que tiene su fundamento constitucional en el artículo 18.4 de la Constitución, interpretado, como demanda su artículo 10.2, a la luz del Convenio n º 108, de 1981, del Consejo de Europa sobre el tratamiento automatizado de datos de carácter personal"[115].

2.7. Marco jurídico de la protección de datos en España

2.7.1. LORTAD

La primera norma sustantiva que reconoce específicamente el derecho a la protección de datos personales en España es la Ley Orgánica 5/1992, de 29

[113] PIÑAR MAÑAS, J.L.: "Protección de datos, origen, situación real y retos de futuro" en *El Derecho a la autodeterminación informativa,* Fundación coloquio jurídico europeo, Ed. San José, Madrid, 2009. Págs. 81 a 179.
[114] MURILLO DE LA CUEVA, P.L.: "El derecho a la libertad informática", en la Base de conocimiento jurídico IUSTEL, www. Iustel.com
[115] MURILLO DE LA CUEVA, P.L, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990

de octubre, *de regulación del tratamiento automatizado de los datos de carácter personal*, ya derogada.

Esa norma, supuso un hito en el reconocimiento del derecho a la protección de datos de carácter personal, siendo la primera en cumplir el mandado del apartado 4º del artículo 18 de la CE, y sentando las bases de las normas posteriores, para las que puede considerarse un antecedente fundamental.

Ese texto normativo, comienza por exponer en su preámbulo como su objetivo es, precisamente: "delimitar una nueva frontera de la intimidad y del honor" que "sustituyendo los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes"; "una frontera, en suma, que garantice que un elemento objetivamente provechoso para la Humanidad no redunde en perjuicio para las personas". "La fijación de esa nueva frontera es el objetivo de la previsión contenida en el artículo 18.4 de la Constitución, y al cumplimiento de ese objetivo responde la presente Ley".

Esa Ley introduce también por primera vez en nuestro ordenamiento el concepto de "tratamiento de datos", que define como "una globalidad de procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados y que son susceptibles, si llegasen a conectarse entre sí, de configurar el perfil personal al que antes se hizo referencia".

Esa norma perseguiría la idea de "implantar mecanismos cautelares que prevengan las violaciones de la privacidad que pudieran resultar del tratamiento de la información", recogiendo de una parte los principios que han generado una *opinio iuris*, definiendo los derechos y garantías atinentes a asegurar la observancia de tales principios generales (preceptos delimitadores del ámbito de aplicación de la Ley, principios reguladores de la recogida,

registro y uso de datos personales y, sobre todo, garantías de la persona); y de otra, la articulación de los extremos concretos que han de regir los ficheros de datos.

Para asegurar la máxima eficacia de sus disposiciones, la Ley encomienda el control de su aplicación a un órgano independiente[116], al que atribuye el estatuto de Ente público en los términos del artículo 6.5 de la *Ley General Presupuestaria*. A tal efecto la Ley configura un órgano especializado, denominado Agencia de Protección de Datos, a cuyo frente sitúa a un Director.

Esa norma no consagra nuevos tipos delictivos, ni define supuestos de responsabilidad penal para la eventualidad de su incumplimiento, al entender que tal cosa deba hacerse, en su caso, en el Código Penal. Sí se atribuye no obstante a la Administración potestad sancionadora, con el fin de que pueda materializar su función de inspección del uso de los ficheros, similar a las demás inspecciones administrativas, y que se configura de distinta forma según se proyecte sobre la utilización indebida de los ficheros públicos (en cuyo caso procederá la oportuna responsabilidad disciplinaria), o sobre los privados (para cuyo supuesto se prevén sanciones pecuniarias).

La Ley disponía un periodo transitorio durante el cual los titulares de ficheros podían adaptarlos a las nuevas exigencias legales. Pasado dicho periodo, comenzaría a aplicarse al ámbito de la protección de datos la protección reforzada de los derechos fundamentales del ciudadano, estableciéndose, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, un "nuevo y más consistente derecho a la privacidad de las personas", en palabras del propio preámbulo de la norma analizada.

[116] A la Agencia Española de Protección de Datos y su estatuto nos referiremos con mayor detenimiento en el Capítulo 6 del presente trabajo.

La LORTAD, es anterior a la Directiva 95/46/CE *de protección de datos de carácter personal*, no obstante lo cual recoge la mayor parte de sus postulados, con la ausencia destacada del derecho de oposición, además de dejar fuera de su ámbito de aplicación algunas ficheros que luego si serían incorporados al ámbito de aplicación de la LOPD[117].

La LORTAD fue desarrollada reglamentariamente a través de los Reales Decretos 428/1993[118], 1332/1994[119] y 994/1999[120], por los que se aprobaron el Estatuto de la Agencia Española de Protección de Datos; se desarrolló parcialmente la LORTAD y se aprobó el Reglamento de medidas de seguridad, respectivamente. Todas esas normas fueron derogadas por la posterior entrada en vigor de la *Ley Orgánica de protección de datos*, que analizaremos en el epígrafe que sigue.

2.7.2. LOPD

El objetivo fundamental de la Ley Orgánica 15/1999, *de protección de datos de carácter personal*[121], fue la trasposición al ordenamiento interno de los postulados de la Directiva 95/46/CE.

---

[117] Ver PIÑAR MAÑAS, ya citado en 70 y 112.
[118] Real Decreto 428/1993, de 26 de marzo*, por el que se aprueba el Estatuto de la Agencia de Protección de Datos*. Publicado en: «BOE» núm. 106, de 4 de mayo de 1993, páginas 13244 a 13250
[119] Real Decreto 1332/1994, de 20 de junio, *por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*. Publicado en: «BOE» núm. 147, de 21 de junio de 1994, páginas 19199 a 19203
[120] Real Decreto 994/1999, de 11 de junio, *por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal*. Publicado en: «BOE» núm. 151, de 25 de junio de 1999, páginas 24241 a 24245.
[121] Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal.*

Con su entrada en vigor se modernizó y adaptó el contenido de la LORTAD al nuevo marco comunitario de protección de datos, ampliando su ámbito de aplicación[122], incrementando asimismo los derechos de los afectados[123], elevando las exigencias de información y consentimiento para recabar y ceder sus datos, reconociendo por vez primera el derecho de oposición, e incluyendo determinadas excepciones a la transferencia internacional de datos.

En particular, la LOPD se dividía en siete títulos:

- el primero es relativo a las disposiciones generales (objeto, ámbito de aplicación y definiciones);

- el segundo, establece los principios de la protección de datos (calidad de los datos; derecho a la información en la recogida de datos; consentimiento del afectado; datos especialmente protegidos; datos relativos a la salud; seguridad de los datos; deber de secreto; comunicación de datos; acceso a los datos por cuenta de terceros)

- el tercero, relativo a los derechos de las personas (impugnación de valoraciones; consulta; acceso; rectificación; cancelación; oposición; rectificación; tutela de derechos y derecho de indemnización);

- el cuarto, que contiene disposiciones sectoriales, está subdividido en dos capítulos y dedica cada uno de ellos a los ficheros de titularidad pública y privada, respectivamente;

[122] Art. 2 LOPD
[123] Título III, artículos 13 a 19: impugnación de valoraciones, derecho de consulta, derechos de acceso, rectificación y cancelación, derecho de oposición, tutela de derechos y derecho de indemnización.

- el título quinto, regula el movimiento internacional de datos, que parte de una prohibición general establecida en el art. 33 de la LOPD, a la que suceden una serie de excepciones a esa prohibición general, que se regulan en el artículo inmediatamente posterior (art. 34). Serían ejemplos: cuando esas transferencias internacionales estén permitidas por convenios internacionales de los que sea parte España; cuando respondan a solicitudes de auxilio judicial; cuando se cuente con el consentimiento del afectado, u otros supuestos similares.

- el sexto, es relativo a la Agencia Española de Protección de Datos. Se establece su naturaleza de ente de derecho público con personalidad jurídica propia, plena capacidad de obrar e independencia, que se regirá, además por lo dispuesto en esa LOPD, por su Estatuto propio. A su frente se situará el Director (art. 36), quien podrá asistirse para el desempeño de las funciones propias de la Agencia (establecidas en el art. 37), de un Consejo Consultivo (art. 38). La AEPD tendrá facultades de inspección y control y contará con un presupuesto propio con cargo a los presupuestos generales del Estado.

- el séptimo y último título tipificaba el régimen de infracciones y sanciones aplicable a los incumplimientos de la normativa en la materia. Estableciendo quienes eran los responsables de esas infracciones, su graduación (leves, graves, muy graves), e importes -desde 100.000 ptas. a 100 millones de pesetas-, plazo de prescripción y procedimiento sancionador.

La LOPD derogó expresamente la LORTAD, estableciendo además en su disposición final primera la habilitación al Gobierno para su desarrollo reglamentario, lo cual se llevó a cabo tiempo después a través del Real Decreto

1720/2007, de 21 de diciembre, *por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*[124].

No obstante, y a pesar de la derogación específica de la ley previa (disposición derogatoria única), la LOPD estableció en su disposición transitoria tercera que el resto de normas reglamentarias preexistentes subsistirían (Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio), "en cuanto no se opongan a la presente Ley" y hasta tanto se llevase a efecto el preceptivo desarrollo reglamentario (2007). Lo cual permite comprender el motivo del lapso de tiempo transcurrido entre la aprobación de la LO 15/1999 y el de su desarrollo reglamentario.

2.7.3 Reglamento de desarrollo de la LOPD. El Real Decreto 1720/2007

El desarrollo reglamentario de la LOPD se produjo a través de distintos Reales decretos anteriores a la propia LOPD (que desarrollaban originalmente la LORTAD pero que habían sobrevivido a su derogación -y que hemos citado en el apartado anterior-), junto con varias Instrucciones de la AEPD (relativas al movimiento internacional de datos[125], publicación de las resoluciones de la AEPD[126] y tratamiento de datos con fines de videovigilancia[127]). Resultaba

[124] BOE» núm. 17, de 19/01/2008.
[125] Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, *relativa a las normas por las que se rigen los movimientos internacionales de datos*. BOE núm. 301, de 16 de diciembre de 2000, páginas 44253 a 44257
https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726
[126] Instrucción 1/2004, de 22 de diciembre, *de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones*. BOE núm. 4 de 5 de enero de 2005.
https://www.boe.es/boe/dias/2005/01/05/pdfs/A00280-00281.pdf
[127] Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, *sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras*. «BOE» núm. 296, de 12/12/2006
https://www.boe.es/buscar/act.php?id=BOE-A-2006-21648

imperativa la adaptación de ese atípico desarrollo reglamentario al contenido de la LOPD.

Según expone el propio Reglamento en su preámbulo, el mismo se aprueba "partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema".

Ese texto reglamentario se estructura en nueve títulos cuyo contenido resumimos seguidamente.

El título I, contempla "el objeto y ámbito de aplicación del reglamento". En particular, se aclara que debe entenderse por "ficheros y tratamientos relacionados con actividades personales o domésticas", considerando la importancia de tal precisión, habida cuenta de que los mismos están excluidos de la normativa sobre protección de datos de carácter personal.

El reglamento no entra a regular el tratamiento de datos de los: a) ficheros regulados por la legislación de régimen electoral; b) los que sirvan a fines exclusivamente estadísticos; c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas; d) los derivados del Registro Civil y del Registro Central de penados y rebeldes; o e) los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia; manteniéndose el régimen jurídico propio de estos tratamientos y ficheros.

También se aportan "un conjunto de definiciones que ayudan al correcto entendimiento de la norma", fijando asimismo "el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados".

El título II, se refiere a los principios de la protección de datos. Regula, por ejemplo, el modo de captación del consentimiento "atendiendo a aspectos muy específicos" como es el caso de los "servicios de comunicaciones electrónicas" y, muy particularmente, "la captación de datos de los menores". Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, con el objeto de clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de los derechos de las personas en el ámbito de la protección de datos de carácter personal. Regula los derechos de acceso, rectificación, cancelación y oposición al tratamiento que, según el Tribunal Constitucional en su sentencia número 292/2000, "constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos" y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que solo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII clarifican aspectos de relevancia para el tráfico ordinario, "como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían - los relativos a la solvencia patrimonial y crédito y los utilizados en actividades

de publicidad y prospección comercial"-, "el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros", "los criterios y procedimientos para la realización de las transferencias internacionales de datos", y, finalmente, "la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos."

El título VIII regula el aspecto de la seguridad, que se considera esencial para la tutela del derecho fundamental a la protección de datos, ya que la misma repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. Según se explica en su exposición de motivos, "el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario". También "ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad" y "regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación".

Finalmente, el título IX se dedica "a los procedimientos tramitados por la Agencia Española de Protección de Datos", optándose por "normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria".

2.7.4 Normativa autonómica de protección de datos

Algunas Comunidades Autónomas han implementado también su propia normativa autonómica de protección de datos.

a) Madrid

En el intervalo temporal entre los años 2001 y 2012, Madrid contó con su propia normativa en materia de protección de datos y también con su propia Agencia Madrileña de Protección de Datos.

La misma se creó a través de la Ley 8/2001, de 13 de julio, *de Protección de Datos de Carácter Personal en la Comunidad de Madrid*[128], y fue derogada por la Ley 8/2012, de 28 de diciembre, *de Medidas Fiscales y Administrativas de la CAM*[129].

El art. 61 de esa última norma acordó la extinción de la Agencia de Protección de Datos de la Comunidad de Madrid, y el reintegro al ámbito estatal de las competencias que le atribuía la Ley 8/2001, correspondiendo nuevamente las mismas a la AEPD.

Durante el tiempo de su vigencia, y de conformidad con lo establecido en el art. 41 de la LOPD, la AMPD ejerció sus funciones sobre los ficheros de datos de carácter personal creados y gestionados por las Instituciones de la Comunidad de Madrid, y para los órganos, organismos, entidades de derecho público y demás entes públicos integrantes de la Administración pública, con excepción de las sociedades mercantiles, así como sobre los ficheros de los Entes que integran la administración local de la CAM.

[128] BOCM de 25 de Julio de 2001
[129] BOCM de 29 de diciembre de 2012, Corrección de errores: (BOCM de 15 de Enero de 2013)

b) Cataluña

La Agencia Catalana de Protección de Datos se crea mediante la Ley 5/2002, de 19 de abril, *de la Agencia Catalana de Protección de Datos*[130]. El objeto de esa ACPD es "velar por el respeto de los derechos fundamentales y las libertades públicas de los ciudadanos en todo lo que concierne a las operaciones realizadas mediante procesos automatizados o manuales de datos personales, dentro del ámbito de actuación que la presente Ley le reconoce, y de acuerdo con las competencias y funciones que le sean encomendadas".

Según disponía su artículo 3, la ACPD "ejerce su autoridad de control sobre los tratamientos de datos personales llevados a cabo por la Generalidad de Cataluña, por los entes que integran la Administración local y por las universidades en el ámbito territorial de Cataluña, por los organismos y las entidades autónomas que dependen de la Administración de la Generalidad o de los entes locales y por los consorcios de los cuales forman parte, de conformidad con lo que establecen la Ley Orgánica 15/1999, de 13 de diciembre, *de protección de datos de carácter personal*, y las disposiciones que la desarrollan".

Asimismo, la Ley autonómica 5/2002 atribuía a la ACDP "competencias con relación a los ficheros creados por las administraciones, los organismos y las entidades a que se refiere el apartado 1 cuando sean gestionados por entidades públicas o privadas en la prestación de servicios públicos, sean o no concesionarias de éstos, o por asociaciones o fundaciones, o por las sociedades civiles o mercantiles en las cuales la Generalidad o los entes locales tengan la participación mayoritaria del capital, cuando llevan a cabo actividades por cuenta de una administración pública". En el criterio de PIÑAR MAÑAS[131],

[130] Publicado en DOGC núm. 3625 de 29 de abril de 2002 y BOE núm. 115 de 14 de mayo de 2002
[131] Citada en 70 y 112.

la citada redacción se extralimitaría claramente de los límites establecidos en el art. 41 de la LOPD.

La aprobación del Estatuto de autonomía de Catalunya en el año 2006 supuso el reconocimiento expreso, por vez primera en el ámbito estatutario, del derecho a la protección de datos, "reforzando el papel de la autoridad de control en materia de protección de datos", "clarificando y ampliando su ámbito de actuación" y, "reforzando su independencia al establecer su designación parlamentaria"[132].

Como consecuencia de las exigencias derivadas de la aprobación del Estatuto de autonomía y otras mejoras técnicas necesarias, se aprueba la Ley 32/2010, de 1 de octubre[133], crea la Autoridad Catalana de Protección de Datos, que deroga la Ley 5/2002.

A través de esa norma se incorporan a la legislación vigente en Cataluña otras modificaciones, como la propia denominación de la autoridad, para evitar la confusión de su naturaleza con el de las entidades de carácter instrumental que bajo la denominación de agencias han aparecido últimamente en el ámbito administrativo.

A través de esa norma se disponen la naturaleza jurídica, ámbito de actuación, organización, funciones y competencias de la Autoridad Catalana de Protección de Datos, entre otras cuestiones, que se subroga en la posición

[132] Preámbulo de la Ley 32/2010.
[133] Ley 32/2010, de 1 de octubre, *de la Autoridad Catalana de Protección de Datos*, «DOGC» núm. 5731, de 08/10/2010, «BOE» núm. 257, de 23/10/2010
https://www.boe.es/buscar/act.php?id=BOE-A-2010-16136

jurídica de la Agencia Catalana de Protección de Datos en cuanto a los bienes, derechos y obligaciones de cualquier tipo de que fuera titular la Agencia[134].

c) País Vasco

El texto normativo de referencia en el ámbito de la Comunidad autónoma del País Vasco es la Ley 2/2004, de 25 de febrero, *de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos*[135].

Su objeto es la regulación de los ficheros de datos de carácter personal creados o gestionados por la Comunidad Autónoma del País Vasco, los órganos forales de los territorios históricos y las administraciones locales de la Comunidad Autónoma del País Vasco, así como la creación y regulación de la Agencia Vasca de Protección de Datos[136].

La regulación de ese organismo se llevó a cabo posteriormente a través del Decreto 308/2005, de 18 de octubre, *por el que se desarrolla la Ley 2/2004, de 25*

[134] El papel de la AEPD, en conexión con el de la ACPD. se reveló relevante al tomar la iniciativa de investigar si la Generalitat de Catalunya cometió alguna ilegalidad en la elaboración del censo del referéndum independentista celebrado el 1/10/2017. La AEPD anunció días antes de esa convocatoria (el 18/09/2017) que había pedido información a distintas instituciones nacionales sobre un posible "acceso ilícito" a sus bases de datos por parte del Govern, y también que le ha solicitado a la Autoridad Catalana de Protección de Datos que haga lo mismo con las instituciones catalanas. La AEPD también subrayó "la ausencia de base legal" para crear "el censo con datos fiscales, médicos, de elecciones pasadas, de padrones municipales, de la Seguridad Social, del registro de población o de la relación de catalanes en el exterior".
MATEO, J.J.: El País, 19/09/2017: "La Agencia de Protección de Datos investiga un posible acceso ilícito para crear el censo electoral catalán"
https://elpais.com/politica/2017/09/18/actualidad/1505734999_480220.html

[135] «BOPV» núm. 44, de 4 de marzo de 2004
«BOE» núm. 279, de 19 de noviembre de 2011
https://www.boe.es/buscar/pdf/2011/BOE-A-2011-18151-consolidado.pdf

[136] http://www.avpd.euskadi.eus/s04-5213/es

de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos[137].

Durante el año 2017, más de 800 consultas se plantearon ante la AVPD, relativas al respeto de la legalidad en materia de protección de datos[138], la mayoría de ellas relativas a consultas sobre "derecho al olvido digital".

d) Andalucía

A través de la Ley 1/2014, de 24 de junio, *de Transparencia Pública de Andalucía*[139], y más concretamente mediante su art. 43, se crea el Consejo de Transparencia y Protección de Datos de Andalucía, que es la autoridad independiente de control en materia de transparencia y protección de datos en esa Comunidad Autónoma. Tiene la consideración de Administración Institucional, por lo que posee personalidad jurídica propia y plena autonomía e independencia en el ejercicio de sus funciones.

Por su parte, los Estatutos del Consejo fueron aprobados por el Decreto 434/2015, de 29 de septiembre[140], en los que se recogen sus reglas de organización y funcionamiento.

La finalidad del Consejo de Transparencia y Protección de Datos de Andalucía es velar por el cumplimiento de la normativa de transparencia pública, tanto

[137] Boletín Oficial del Pais Vasco de 16-11-2005
[138] https://www.noticiasdegipuzkoa.eus/2018/07/16/sociedad/euskadi-recibe-mas-de-800-consultas-sobre-proteccion-de-datos
[139] BOJA nº 124 de 30/06/2014
https://www.juntadeandalucia.es/boja/2014/124/1
[140] Decreto 434/2015, de 29 de septiembre, *por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía.* BOJA nº 193 de 02/10/2015
https://www.juntadeandalucia.es/boja/2015/193/1

en lo que se refiere a publicidad activa como a la defensa y salvaguarda del derecho de acceso a la información pública, velando asimismo por el cumplimiento de la normativa de protección de datos en al ámbito de sus competencias (fundamentalmente, ficheros de titularidad pública autonómicos).

Respecto de la materia objeto de examen, el art. 45 de la Ley 1/2014 citada dispone: "El Consejo actuará en el territorio de Andalucía como autoridad pública independiente de control en materia de protección de datos en los términos previstos en el artículo 41 de la Ley Orgánica 15/1999, de 13 de diciembre, y como órgano independiente e imparcial garante del derecho a la transparencia, conforme a lo previsto en esta ley y en la legislación básica en la materia".

2.7.5 Leyes sectoriales con incidencia en la protección de datos

Son ejemplos de leyes sectoriales con incidencia en la materia de la protección de datos tanto la Ley 34/2002, de 11 de julio, *de servicios de la sociedad de la información y de comercio electrónico*[141], como la Ley 9/2014, de 9 de mayo, *General de Telecomunicaciones*[142].

Ambas incluyen en su articulado medidas específicas que garantizan la protección de los derechos de los interesados respecto de la protección de sus

[141] «BOE» núm. 166, de 12/07/2002.
https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
[142] «BOE» núm. 114, de 10/05/2014.
https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

datos de carácter personal en relación con las materias objeto de esa normativa sectorial[143].

[143] Por ejemplo, el art. 42 de la LGT dispone que "los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar la protección de los datos de carácter personal".
Lo mismo sucede en el art. 22 de la LSSI, que establece las obligaciones que deben cumplir los prestadores de esos servicios para respetar los derechos de los destinatarios de esos servicios.

CAPÍTULO 3

LA CONSAGRACIÓN DEL DERECHO AL OLVIDO POR EL TJUE: LA SENTENCIA GOOGLE C./ ESPAÑA Y SU IMPACTO.

SUMARIO: 3.1 LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (GRAN SALA), DE 13 DE MAYO DE 2014 EN EL ASUNTO C- 131/12, EN EL PROCEDIMIENTO ENTRE GOOGLE ESPAÑA, S. L., GOOGLE INC. CONTRA LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y MARIO COSTEJA GONZÁLEZ; 3.1.1. INTRODUCCIÓN; 3.1.2 LAS CUESTIONES PREJUDICIALES ELEVADAS AL TRIBUNAL DE JUSTICIA DE LA UE; A.) RESPUESTAS DEL TJUE RESPECTO DE LA SEGUNDA CUESTIÓN PREJUDICIAL: ACTIVIDAD DE LOS BUSCADORES COMO PROVEEDORES DE CONTENIDOS; B.) RESPUESTAS DEL TJUE RESPECTO DE LA PRIMERA CUESTIÓN PREJUDICIAL: SOBRE EL ÁMBITO DE APLICACIÓN DE LA DIRECTIVA 95/46; C.) RESPUESTAS DEL TJUE A LA CUESTIÓN PREJUDICIAL RELATIVA AL ALCANCE DEL DERECHO DE CANCELACIÓN Y/OPOSICIÓN EN RELACIÓN CON EL DERECHO AL OLVIDO; 3.2 IMPACTO DE LA SENTENCIA GOOGLE EN EL MARCO DE LA UE; 3.2.1 DIRECTRICES DEL GRUPO DE TRABAJO DEL ART. 29; 3.2.2 THE ADVISORY COUNCIL TO GOOGLE; 3.3. LA REPERCUSIÓN DE LA SENTENCIA GOOGLE EN ESPAÑA; 3.3.1 LA SENTENCIA DE LA SECCIÓN 1º DE LA SALA DE LO CONTENCIOSO-ADMINISTRATIVO DE LA AUDIENCIA NACIONAL, DE 29 DE DICIEMBRE DE 2014; A.) RESPECTO DE LA ACTIVIDAD DEL MOTOR DE BÚSQUEDA; B.) SOBRE LA APLICACIÓN TERRITORIAL DE LA DIRECTIVA 45/96/CE Y LA NORMATIVA NACIONAL DE PROTECCIÓN DE DATOS; C.) SOBRE LA ALEGADA FALTA DE LEGITIMACIÓN PASIVA POR PARTE DE GOOGLE SPAIIN; D.)PUNTUALIZACIONES FORMULADAS EN LA SENTENCIA SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS Y LIBERTADES DE EXPRESIÓN E INFORMACIÓN; E.) LOS CRITERIOS DE PONDERACIÓN; F.) APLICACIÓN DE LOS CRITERIOS DE PONDERACIÓN AL CASO; G.) INTERPRETACIÓN DE LA RESOLUCIÓN DE LA AEPD; 3.3.2. LA SENTENCIA DE LA SECCIÓN 6ª DE LA SALA DE LO CONTENCIOSO-ADMINISTRATIVO DEL TRIBUNAL SUPREMO, NÚM. 1611/2016 DE 4 JULIO; 3.3.3 INTERROGANTES SOBRE LA APLICACIÓN DE LA SENTENCIA GOOGLE.

3.1. La Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 13 de mayo de 2014, en el Asunto C- 131/12, procedimiento entre Google España, S. L., Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González

3.1.1. Introducción

El TJUE se pronunció por vez primera sobre el alcance y límites del derecho al olvido digital en su Sentencia de 13 de mayo de 2014, dictada en el asunto C-131/12, en el

procedimiento entre Google España S.L., Google Inc. Vs. AEPD y Mario Costeja González (en adelante, *Google vs. España* o *Sentencia Google*)[144].

La Sentencia[145], es uno de los asuntos con mayor transcendencia social y repercusión jurídica de los últimos años[146][147], y ha sido objeto de numerosos estudios doctrinales y comentarios[148][149][150].

El supuesto de hecho que se analiza en la misma es el siguiente: en el año 1998, el periódico "La Vanguardia" publicó dos anuncios relativos a una subasta de inmuebles en los que se citaba al embargado con nombre y apellidos. Esa subasta estaba relacionada con deudas de la Seguridad Social. Con posterioridad a esa fecha, el medio digitalizó su hemeroteca, y esa noticia se puso a disposición del público a través de Internet.

En el mes de noviembre de 2009, el Sr. Costeja contactó con el periódico "La Vanguardia" ejercitando su derecho de oposición al tratamiento de sus datos de carácter personal, alegando que al introducir su nombre y apellidos en el buscador de Internet Google, entre los resultados arrojados se encontraba el de la noticia publicada en 1998, y ello a pesar de tratarse de un asunto arreglado y zanjado hacía muchos años y que en el año 2009 carecía de interés.

---

144 http://curia.europa.eu/juris/liste.jsf?language=es&num=C-131/12
145 RALLO, A.: *El derecho al olvido en Internet. Google vs. España*. Colección "cuadernos y debates", Centro de Estudios Políticos y Constitucionales, Madrid, 2014. Págs. 34 y ss., ya citado.
146 HERNÁNDEZ RAMOS, M., "Motores de búsqueda y derechos fundamentales en Internet: La STJUE Google C-131/12, de 13 de mayo de 2014", *Revista General de Derecho Europeo* núm. 34, Ed. Iustel. ISSN: 1696-9634, núm. 34, Octubre (2014) https://www.iustel.com//v2/revistas/detalle_revista.asp?id=13&numero=34&
147 ÁLVAREZ CARO, M.: *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Editorial Reus, Madrid, 2015.
148 GUICHOT, E.: "El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español", *Revista de Administración Pública*, 209, 45-92.
149 SORIANO GARCÍA, J.E.: "Presente del derecho al olvido". *El Cronista del Estado Social y Democrático de Derecho*, ISSN 1889-0016, Nº. 78, 2018, págs. 4-21.
150 BERROCAL LANZAROT, A.: *Derecho de supresión de datos o derecho al olvido*. Colección jurídica general. Monografías. Ed. Reus, S.A. Madrid, 2017.

El medio desatendió la reclamación del Sr. Costeja, al entender que esa publicación se había hecho en su día por orden del Ministerio de Trabajo y Asuntos Sociales. Mario Costeja reprodujo la solicitud ante Google España, quien respondió reenviando al Sr. Costeja ante Google Inc., aludiendo que esa empresa americana es quien presta el servicio de buscadores.

Mario Costeja se dirigió entonces a la Agencia Española de Protección de Datos, formulando una reclamación ante La Vanguardia, Google España y Google Inc. que fue estimada mediante resolución de fecha 30 de julio de 2010 (R/01515/2010, de 30 de julio de 2010)[151]. En esa resolución, la Agencia Española de Protección de Datos estimó la reclamación frente a Google España y Google Inc. pero la rechazó contra La Vanguardia, al entender que la publicación en dicho medio tendría justificación legal. Tanto Google España como Google Inc. recurrieron esa resolución ante la Sala de lo contencioso-administrativo de la Audiencia Nacional.

3.1.2 Las cuestiones prejudiciales elevadas al Tribunal de Justicia de la UE

Mediante Auto de fecha 27 de febrero de 2012, núm. 19/2012 (dictado en el recurso 725/2010), la Audiencia Nacional acotó el objeto de controversia a "determinar las obligaciones que tienen los gestores de los motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información publicada en páginas web de terceros, que contienen sus datos personales y permite relacionarles con la misma, sea localizada, indexada y puesta a disposición de los internautas de forma indefinida".

[151] https://www.aepd.es/resoluciones/TD-00650-2010_REC.pdf

Al considerar que la interpretación de esta cuestión dependía de la que se hiciera de la Directiva 95/46 *de Protección de Datos de las Personas Físicas*, la Sección 1ª de la Sala de lo contencioso-administrativo de la Audiencia Nacional acordó formular nueve cuestiones prejudiciales de interpretación ante el Tribunal de Justicia de la Unión Europea, que se dividen a su vez en tres bloques diferenciados, y que se recogen en el citado Auto de 27 de febrero de 2012. A saber:

> *"1. Por lo que respecta a la* ***aplicación territorial*** *de la Directiva 95/46/CE y, consiguientemente de la normativa española de protección de datos:*
>
> > *1.1 ¿Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE, cuando concurra alguno o algunos de los siguientes supuestos:*
> >
> > - *cuando la empresa proveedora del motor de búsqueda crea en un Estado Miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado, o*
> >
> > - *cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa o*
> >
> > - *cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de*

protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?

1.2 ¿Debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un "recurso a medios situados en el territorio de dicho Estado miembro" cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro?.

1.3 ¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en Internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas?

1.4. Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considerase por el Tribunal de Justicia de la Unión que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, ¿Debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta europea de derechos fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea?

2. Por lo que respecta a la ***actividad de los buscadores como proveedor de contenidos*** *en relación con la Directiva 95/46/CE de Protección de Datos:*

2.1. En relación con la actividad del buscador de la empresa "Google" en Internet, como proveedor de contenidos, consistente en localizar la información publicada o

incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas, ¿Debe interpretarse una actividad como la descrita comprendida en el concepto de "tratamiento de datos" contenido en el art. 2.b de la Directiva 95/46/CE?

2.2. En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita: ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador "Google" es "responsable del tratamiento" de los datos personales contenidos en las páginas web que indexa?

2.3. En el caso de que la respuesta anterior fuera afirmativa: ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa "Google" para exigirle la retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información?

2.4. En el caso de que la respuesta a esta última pregunta fuera afirmativa, ¿Se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

3. Respecto al ***alcance del derecho de cancelación y/oposición en relación con el derecho al olvido*** *se plantea la siguiente pregunta:*

> *3.1. ¿Debe interpretarse que los derechos de supresión y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?"*

El primer bloque de preguntas viene referido, como hemos visto, a la aplicación territorial de la Directiva. El segundo, alude a si los buscadores de Internet, cuando indexan contenidos, están realizando una actividad sujeta a la normativa de protección de datos. Y el tercer y último bloque, se refiere a si el derecho de supresión o cancelación debe entenderse como el derecho del particular cuyos datos se indexan a borrarlos cuando su captación y puesta a disposición del público ya no está justificada por fines de interés general.

Esas preguntas fueron respondidas en la aludida Sentencia del TJUE de 13 de mayo de 2014 de la forma que sigue[152]:

[152] Respuesta radicalmente opuesta a las conclusiones formuladas por el Abogado General, NIILO JÄÄSKINEN en ese procedimiento, publicadas con fecha de 25 de junio de 2013, y en las que abogaba por que el TJUE determinase la irresponsabilidad del proveedor de servicios respecto de los resultados arrojados por los motores de búsqueda y la inexistencia de un derecho del interesado a solicitar al desindexación de los resultados (olvido).
http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES

a.) Respuestas del TJUE respecto de la segunda cuestión prejudicial: actividad de los buscadores como proveedores de contenidos

1ª./ Respecto de la cuestión sobre "si el artículo 2, letra b), de la Directiva 95/46[153] debe examinarse en el sentido de que la actividad de un motor de búsqueda como proveedor de contenidos", "que consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado" entiende el TJUE que "debe calificarse de «tratamiento de datos personales», en el sentido de dicha disposición", "cuando esa información contiene datos personales".

El Tribunal resuelve esa cuestión de forma afirmativa en el numeral 28 de esa resolución judicial, subrayando que "al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica", "el gestor de un motor de búsqueda «recoge» tales datos que «extrae», «registra» y «organiza» posteriormente en el marco de sus programas de indexación, «conserva» en sus servidores y, en su caso, «comunica» y «facilita el acceso» a sus usuarios en forma de listas de resultados de sus búsquedas". Y que como esas operaciones están contempladas de forma "explícita e incondicional" en el artículo 2, letra b), de la Directiva 95/46, la actividad descrita debe calificarse de «tratamiento» en el sentido de dicha disposición, "sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales".

[153] La letra b) del artículo 2º de esa Directiva dice así: "*b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción".*

2./ Asimismo también resuelve que, al ser el gestor de búsqueda quien "determina los fines y los medios de esa actividad" y el tratamiento de datos se realiza en el marco de esta, el gestor del motor de búsqueda debe considerarse «responsable» de dicho tratamiento en virtud del mencionado artículo 2, letra d) de la Directiva 95/46[154].

3./ Respecto de la cuestión relativa a si una autoridad nacional puede requerir directamente a un motor de búsqueda la desindexación de determinada información, o si es preciso pasar primero por un requerimiento al medio en cuestión, responde el TJUE que es posible requerir directamente al responsable de tratamiento del motor de búsqueda, al amparo de lo establecido en los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46[155], quien "debe entonces examinar debidamente su fundamento y, en su caso, poner fin al tratamiento de los datos controvertidos".

A lo anterior, añade también el TJUE que "no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet". Y que para el caso de que un responsable del tratamiento no acceda a las solicitudes, "el interesado puede acudir a la autoridad de control o a los tribunales para que éstos lleven a cabo las comprobaciones necesarias y ordenen a dicho gestor las medidas precisas".

---

[154] La letra d) de ese artículo 2º dice: *"d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario"*;

[155] La letra a) del art. 14 de la Directiva 95/46 dice así: *Los Estados miembros reconocerán al interesado el derecho a: "a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos";*

Concluyendo: "para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web, y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita".

b.) Respuestas del TJUE respecto de la primera cuestión prejudicial: sobre el ámbito de aplicación de la Directiva 95/46

1./ El TJUE comienza recordando como el considerando 19 de la Directiva de protección de datos dispone que «el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable», y «que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante».

2./ Respecto de esos dos requisitos subraya que "Google España se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España" (esa actividad sería la promoción y venta de espacios publicitarios) y que tiene "personalidad jurídica propia", por lo que, "es un establecimiento", en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46[156]".

[156] La letra a) del apartado 1º del art. 4 de la Directiva reza: *"1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable".*

3./ Sobre la necesidad de que, además de poseer un establecimiento en el Estado miembro, el tratamiento de datos personales por parte del responsable del tratamiento "se lleve a cabo en el marco de las actividades de un establecimiento de dicho responsable situado en territorio de un Estado miembro" concluye el Tribunal que el artículo 4, apartado 1, letra a) de la Directiva 95/46 debe interpretarse en el sentido de que "el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa "en el marco de las actividades» de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor".

Y ello considerando:

A) que ese artículo no exige que el tratamiento de datos en cuestión sea efectuado "por" el propio establecimiento en cuestión, sino que se realice "en el marco de las actividades de éste" (posición sostenida por el Gobierno español) y

B) que el objetivo de la Directiva es garantizar una protección a los derechos fundamentales de los ciudadanos de la Unión Europea frente a injerencias de terceros, lo cual exige que esa protección se interprete de forma extensa y sin restringir su ámbito de aplicación territorial. Otra cosa haría imposible los objetivos de la Directiva, que podrían ser burlados mediante el establecimiento en un país tercero y no miembro de la UE.

c.) *Respuestas del TJUE a la cuestión prejudicial relativa al alcance del derecho de cancelación y/oposición en relación con el derecho al olvido*

El Tribunal de Justicia de la Unión Europea concluye[157] que la cuestión relativa al alcance del derecho de cancelación y oposición respecto del derecho al olvido debe responderse en el sentido de que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que resulta preciso realizar un análisis pormenorizado, en el que se examine si el interesado podría tener derecho a que una determinada información relativa a su persona deje de estar vinculada a su nombre, por causarle un perjuicio o ser irrelevante en el momento actual. Ese derecho prevalecería frente a los intereses económicos del gestor del motor de búsqueda, y también sobre el interés del público a acceder a esa información partiendo del nombre de una determinada persona. No obstante, podría suceder, que en supuestos en los que la persona interesada tenga relevancia, por ocupar un cargo en la vida pública, prevalezca el interés del público a tener información sobre esa persona sobre el interés del individuo a que sus datos se eliminen de la lista de resultados.

La decisión del Tribunal de Justicia de la Unión Europea acoge los argumentos sostenidos por el denunciante y por el Gobierno español, al entender que el interés de la persona física afectada por el tratamiento prevalece frente a otros intereses, como lo son la libertad informativa o los intereses económicos del gestor del motor de búsqueda. No lo entendían así los responsables de Google y algunos otros Gobiernos de Estados miembros de la UE personados en las actuaciones (Grecia; Austria; Polonia), quienes sostenían que ese tratamiento solo podía impedirse por motivos tasados y contemplados de forma expresa en la Directiva, pero no por la mera consideración de que unos datos pudieran perjudicarles y quieran que los mismos sean olvidados.

[157] Apartado 99 de la Sentencia.

> En el criterio del TJUE, la incompatibilidad de los datos con los fines de la Directiva puede venir dada por el hecho de que los datos no solo sean inexactos, sino que también sean "inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento", de que "no estén actualizados" o de que "se conserven durante un período superior al necesario", a menos que se imponga su conservación por fines históricos, estadísticos o científicos[158]. Pudiendo suceder asimismo que unos datos que originalmente habían sido publicados de forma correcta, devengan excesivos como consecuencia del paso del tiempo, resultando ahora innecesarios para los fines para los que inicialmente fueron recogidos o resulten en la actualidad excesivos, debiendo ser retirados.

3.2 Impacto de la Sentencia Google en el marco de la UE

A raíz del dictado de la S*entencia Google*, la compañía puso a disposición de los usuarios un formulario para solicitar la retirada de información personal https://support.google.com/legal/contact/lr_eudpa?product=websearch Esto mismo han hecho también otros buscadores mayoritarios como Bing[159] o Yahoo[160].

Desde el 29 de mayo de 2014 y hasta el mes de agosto de 2019 (5 años), Google ha recibido más de 800.000 solicitudes de desindexación (834.733)[161], que afectaban a 3.281.701 URL, de las que ha suprimido 1.199.955 –el 44,5% de las peticiones–. De todas estas, el 88,6% las habían promovido personas particulares; el resto correspondían a menores de edad, entidades corporativas, políticos y personas con

[158] Apartado 92 de la Sentencia.
[159] https://www.bing.com/webmaster/tools/eu-privacy-request
[160] https://guce.oath.com/collectConsent?sessionId=3_cc-session_3bf1d079-e198-4211-8b81-4c854b868de2&lang=&inline=false&jsVersion=null&experiment=null
[161] https://transparencyreport.google.com/eu-privacy/overview, a 17/8/2019.

cargo o relevancia pública. De esas más de 800.000 solicitudes, 79.710 se realizaron desde España, e incumbían a 261.125 URL[162]. De esas solicitudes, el buscador ha suprimido 81.813 enlaces, el 37,9%.

En la evaluación de esas solicitudes, Google debe realizar un balance entre los derechos del usuario y el interés público que, en su caso, pudiera suscitar el contenido. El sitio web más afectado por esas solicitudes es Facebook, con 47.418 urls.[163]

3.2.1. Directrices del Grupo de trabajo del art. 29

Además de lo anterior, cabe destacar, que a raíz del dictado de la Sentencia del TJUE, el Grupo de trabajo del art. 29[164], procuró establecer las condiciones que debían tenerse en cuenta para aplicar el denominado derecho al olvido en Internet, y en particular a la hora de efectuar un balance lo más objetivo posible entre ese derecho al olvido y el derecho a la información.

En particular, el 26 de noviembre de 2014, ese Grupo de trabajo del art. 29 publicó unas directrices para la implementación de la aludida *Sentencia Google España*[165]. En ese documento, con una extensión de 20 páginas, se realiza en primer término un análisis del contenido de la *Sentencia Google* (cómo debe entenderse el concepto de "motor de búsqueda"; forma en la que deben ejercitarse los derechos por parte de los interesados; ámbito de aplicación; comunicación a terceros sobre el ejercicio del derecho al olvido); para

[162] https://transparencyreport.google.com/eu-privacy/overview?requests_over_time=country:ES&lu=requests_over_time a 17/8/2019
[163] Fuente, informe transparencia GOOGLE.
[164] *El Grupo de trabajo del artículo 29 (GT Art. 29) es el grupo de trabajo europeo independiente que se ha ocupado de cuestiones relacionadas con la protección de la privacidad y los datos personales hasta el 25 de mayo de 2018 (entrada en aplicación del RGPD). Se pueden consultar aquí todas las noticias archivadas sobre el (GT Art. 29). Fuente: European Data Protection Board: https://edpb.europa.eu/our-work-tools/article-29-working-party_es*
[165] http://www.dataprotection.ro/servlet/ViewDocument?id=1080

seguidamente, en la segunda parte del mismo, establecer un compendio de 13 directrices para la aplicación de esa Sentencia en el día a día de los responsables de los buscadores, aportando soluciones estandarizadas a problemas comunes:

- Por ejemplo, en el criterio del Grupo de trabajo del art. 29, a pesar de que la *Sentencia Google* alude solo a las búsquedas que pudieran formularse a través del concreto nombre y apellidos de una persona, entiende relevantes también las que pudieran hacerse a través de apodos o pseudónimos, siempre que los mismos estén vinculados a la identidad de la persona permitiendo su reconocimiento.

- Establece una posible justificación para oponerse al borrado de la información o a la exclusión del nombre de la persona del motor de búsqueda, el hecho de estar esa persona vinculada a la "vida pública" o tratarse de "figuras públicas". Subraya el Grupo de trabajo en las Directrices analizadas la dificultad de establecer de antemano una definición única para todos ellos, pero viene a decir que podrá entenderse incluido aquél quien, en el desarrollo de sus funciones, tenga un cierto grado de exposición al público.

- Se puntualiza en esas directrices que, en el caso de que la información cuya eliminación se solicita venga referida a un menor, será siempre prevalente el mejor interés de éste, en aplicación del art 24[166] de la *Carta de derechos fundamentales de la Unión Europea*.

[166] *Artículo 24- Derechos del menor:*

1. Los menores tienen derecho a la protección y a los cuidados necesarios para su bienestar. Podrán expresar su opinión libremente. Ésta será tenida en cuenta en relación con los asuntos que les afecten, en función de su edad y de su madurez.

2. En todos los actos relativos a los menores llevados a cabo por autoridades públicas o instituciones privadas, el interés superior del menor constituirá una consideración primordial.

- Respecto de la exactitud de los datos, interpreta el Grupo de trabajo que esa exactitud debe venir referida a hechos, no a opiniones, y que en el caso de estar la exactitud de esos hechos sujeta a decisión judicial, lo más adecuado será esperar a la resolución de la controversia para decidir la procedencia, o no, de su eliminación.

- En cuanto a si un concreto dato debe considerarse, o no, excesivo, el Grupo de trabajo aconseja que en el balance entre los derechos en conflicto se tengan en cuenta cuestiones tal y como si un determinado dato hace referencia la vida profesional o privada del reclamante, si se trata de una opinión contraria al reclamante o si esa opinión llega incluso a incitar al odio o no. En el caso de las opiniones, el GT29 argumenta la falta de competencia de las Autoridades Nacionales de protección de datos, sugiriendo que el reclamante sea reenviado a las jurisdicciones civil o penal para que solicite en ese contexto la retirada.

- Respecto de la "información sensible" o los "datos especialmente protegidos" (religión, salud, sexualidad), entiende que, en principio, las reclamaciones deben ser acogidas y la tendencia de las Autoridades de protección de datos debe ser la intervención.

- Sobre si la información publicada está o no actualizada, el Grupo de trabajo subraya la importancia de que las Autoridades Nacionales garanticen que la información publicada esté puesta al día, de tal forma que la misma no se haya desactualizado por el paso del tiempo y, consecuentemente, sea en la actualidad imprecisa.

3. Todo menor tiene derecho a mantener de forma periódica relaciones personales y contactos directos con su padre y con su madre, salvo si son contrarios a sus intereses

- Respecto a la circunstancia de si la información publicada causa, o no, perjuicio al interesado, concluye el GT29 que no es preciso que esa información "cause perjuicio" al reclamante, pero si se presumirá que ese perjuicio existe si los datos tienen un impacto negativo excesivo, revelan aspectos triviales, o vienen referidos a hechos que han dejado de ser objeto de debate público.

- Los responsables de los motores deberán considerar también el borrado de datos personales en el supuesto de que los mismos puedan poner en peligro a los afectados, como por ejemplo, facilitando la usurpación de su identidad

3.2.2. The advisory Council to Google

Por su parte, ante el desafío que para la compañía suponía tener que hacer frente a miles de solicitudes de desindexación, y con el objeto de implementar las obligaciones impuestas por el TJUE de la mejor manera posible, Google buscó el asesoramiento de expertos sobre los principios a aplicar en casos individuales. Así, conformó un consejo de expertos que se reunieron en varias sesiones en distintos lugares de Europa, publicando sus conclusiones y recomendaciones en un Informe[167].

En ese Informe se establecían ciertos criterios objetivos en función de los cuales poder abordar las solicitudes de desindexación sobre la base de criterios más o menos uniformes. Particularmente, los expertos aconsejaban a Google tener en cuenta los siguientes parámetros a la hora de abordar esas solicitudes

[167] The Advisory Council to Google on the right to be forgotten https://static.googleusercontent.com/media/archive.google.com/es//advisorycouncil/advisement/advisory-report.pdf

de desindexación. 1) el carácter público, o no, del solicitante; 2) la naturaleza de la información, el grado de injerencia de esa información en la vida privada del reclamante y su relevancia, o no, para la opinión pública; 3) la fuente de la información y su fiabilidad; o 4) el tiempo transcurrido desde la publicación.

Asimismo, se sugiere en ese documento la implementación de un protocolo de desindexación que incluyese notificaciones sobre esa solicitud a los responsables de los sitios web en los que se publique la información comprometida, el ámbito geográfico para la atención de las solicitudes o la transparencia sobre los resultados de las solicitudes y su estimación/desestimación.

3.3. La repercusión de la Sentencia GOOGLE en España

Ya hemos señalado como, según datos publicados en el portal de transparencia de la propia Google, el porcentaje de solicitudes atendidas en España se encuentra en el 38% del total, y levemente por debajo de las atendidas en el marco de la UE, que serían el 44%.

Según datos publicados por la propia Agencia Española de Protección de Datos en su séptima sesión abierta celebrada con fecha de abril de 2015, la Sentencia del TJUE Google vs. España (Costeja), de 13 de mayo de 2014, dio lugar, solo en el año inmediatamente posterior a su promulgación (hasta abril de 2015), a setenta y dos sentencias de la Audiencia Nacional, de las cuales 54 fueron desestimatorias de los recursos interpuestos frente a las Resoluciones de la AEPD (75%), 14 estimatorias (19%), y 4 parcialmente estimatorias (6%)[168]. Frente a esas Sentencias de la Sala de lo contencioso-administrativo de la Audiencia Nacional solo se interpusieron 9 recurso

[168] Los datos son de la Agencia Española de Protección de Datos, y han sido publicados en la "7ª Sesión Anual abierta" de ese organismo, celebrada el 29 de abril de 2015..

de casación ante la Sala de lo contencioso administrativo del Tribunal Supremo, estimándose esos recursos solo en dos de los nueve supuestos sometidos al enjuiciamiento de ese Tribunal.

El diario El País publicó el 3 de abril de 2018 bajo el titular "64.000 españoles quieren ser olvidados"[169], que "desde 2014, Google ha recibido en los países de la UE 656.899 solicitudes para retirar del buscador más de 2,4 direcciones de Internet de las que ha cancelado alrededor de un millón". De esas solicitudes, 64.000 se formularon desde España, habiéndose atendido el 38%.

Entre las reclamaciones atendidas se encuentra, por ejemplo, la de una persona que figuraba en un registro policial como culpable de haber atropellado mortalmente con su vehículo a una persona hacía cincuenta años, y que Google estimó en atención al lapso de tiempo transcurrido desde el momento en que los hechos habían sucedido y hasta la actualidad. No accedió, por el contrario, a borrar una información publicada en 2004 relativa a una persona que había formado parte del brazo político de una organización terrorista, entendiendo que en ese supuesto primó el interés público, por lo que la información se mantuvo en la web.

Con carácter general, Google mantiene las informaciones si las mismas aluden a personajes públicos o son informaciones avaladas por documentos oficiales (informes policiales, sentencias), accediendo a retirarlas, en estos últimos supuestos, solo si media una orden de la autoridad nacional de protección de datos correspondiente.

De todos esos procedimientos, el más relevante fue el que, una vez resueltas las cuestiones prejudiciales resolvió el conflicto surgido entre Google, el Sr. Costeja y la Agencia Española de Protección de Datos, por ser el primero que aplicó la fundamentación contenida en la Sentencia del TJUE.

[169] Diario El País, Ed. Madrid, 3 de abril de 2018, página 23: "64.000 españoles quieren ser olvidados: aumentan las peticiones a la plataforma para retirar del buscador direcciones de Internet".

3.3.1 La Sentencia de la Sección 1º de la Sala de lo contencioso-administrativo de la Audiencia Nacional, de 29 de diciembre de 2014

La Sentencia de la Sección 1ª de la Sala de lo contencioso-administrativo de la Audiencia Nacional, de 29 de diciembre de 2014, dictada en el recurso 725/2010[170], resuelve el recurso contencioso administrativo interpuesto por Google España y Google Inc. frente a la Resolución de la Agencia Española de Protección de Datos de 30 de julio de 2010.

Como ya se ha explicado en un apartado anterior del presente Capítulo (3.1.2 pág. 107), por Auto de esa Sala de 27 de febrero de 2012 se acordó plantear al TJUE cuestión prejudicial de interpretación, al amparo del artículo 267 del Tratado de Funcionamiento de la Unión Europea, sobre: 1) aplicación territorial de la Directiva 95/46/CE; 2) actividad de los buscadores como proveedores de contenidos a la luz de las disposiciones de la Directiva 95/46/CE; y 3) alcance del derecho de cancelación y/oposición en relación con el derecho al olvido.

A esas cuestiones dio respuesta el TJUE (Gran Sala), mediante Sentencia de 13 de mayo de 2014, asunto C-131/2012, Google España, S.L. y Google Inc./AEPD, en el sentido expresado en el presente Capítulo.

Esa Sentencia del TJUE se recibió por la Sala de lo contencioso-administrativo de la Audiencia Nacional mediante providencia de 28 de mayo de 2014, alzándose la suspensión de las actuaciones, y concediéndose a las partes un plazo por veinte días a fin de que alegasen lo que entendieren pertinente sobre el contenido de la citada resolución judicial. Las partes presentaron en tiempo y forma los correspondientes escritos, resolviendo la Audiencia Nacional mediante la Sentencia a la que aludimos, desestimar el recurso interpuesto por Google España y Google Inc., declarando la

[170] http://www.poderjudicial.es/search/openCDocument/d6c3141dd81d8758a0bb78e44820713e83b1b8ed4f7b05ec

adecuación a Derecho de la Resolución de tutela de derechos de la AEPD impugnada, sin imponer las costas procesales a ninguna de las partes.

Los razonamientos contenidos en esa Sentencia de la Audiencia Nacional, recogen los del TJUE en Sentencia de 13 de mayo de 2014, dedicando sus cinco primeros fundamentos de derecho a reproducir los antecedentes de hecho de la resolución de la Agencia (F.Dº1), los argumentos contenidos en las demandas de Google España, S.L (F.Dº2). y Google Inc. (F.Dº3); los de las partes demandadas (Abogacía del Estado y Sr. Costeja -F.Dº4-); y las alegaciones formuladas en el trámite concedido con ocasión del planteamiento de las cuestiones prejudiciales ante el TJUE (F.Dº5).

Es a partir del fundamento de derecho sexto de esa resolución judicial cuando se abordan las cuestiones planteadas ante el Tribunal de Justicia de la Unión Europea y se rebaten los argumentos sostenidos por las demandantes en sus escritos, y en particular: la actividad del motor de búsqueda (F.Dº6); la aplicación territorial de la norma (F.Dº7); falta de motivación de la resolución (F.Dº8); falta de legitimación pasiva de Google España, S.L. (F.Dº9); indefensión alegada por Google Inc. (F.Dº10); libertad de empresa (F.Dº11); Derecho a la protección de datos y libertades de expresión e información (F.Dº12); exposición de los criterios de ponderación contenidos en la Sentencia del Tribunal de Justicia (F.Dº13); aplicación de esos supuestos al caso concreto (F.Dº14); interpretación del contenido de la resolución de la Agencia (F.Dº15); pronunciamiento final sobre las costas (F.Dº16).

Analizamos seguidamente los más relevantes de todos ellos:

a.) Respecto de la actividad del motor de búsqueda.

La Sala hace suyos los razonamientos del Tribunal de Justicia relativos a la actividad del motor de búsqueda, considerando que "ninguna duda cabe que la actividad de un motor de búsqueda como proveedor de contenido debe

calificarse de "tratamiento de datos personales" y que, en tal concepto, es asimismo un "intermediario de la sociedad de información" según la Ley 34/2002, de 11 de julio.

La Sala descarta los argumentos de las recurrentes según los cuales los buscadores deben considerarse meros intermediarios de la sociedad de la información, por lo que no les sería aplicable la aludida Ley 34/2002 y tampoco serían responsables del tratamiento. En el criterio de la Audiencia Nacional son ajustados a derecho los argumentos contenidos en la resolución recurrida, según los cuales "los buscadores en el ejercicio de su actividad, efectúan un tratamiento de datos de carácter personal por lo que están obligados a hacer efectivo el derecho de cancelación y/oposición del interesado que no desea que se indexe y sea puesta a disposición de los internautas determinada información a él referida que se encuentra en páginas de tercero y permiten relacionarles con la misma" estando asimismo obligados a "cumplir con los requerimientos que les dirija la AEPD en la tutela de esos derechos".

También dispone que, los datos personales obtenidos por el buscador, que es un intermediario de la Sociedad de la Información, pueden afectar a la dignidad de las personas y lesionar derechos de un tercero, por lo que el Director de la AEPD, como órgano competente para velar por el cumplimiento de la legislación de datos y controlar su aplicación, puede requerir al responsable del tratamiento de los datos, la adopción de medidas necesarias para la adecuación del tratamiento de los datos a las disposiciones de la Ley Orgánica 15/1999, ejerciendo las facultades que le atribuye su artículo 37, así como a los efectos establecidos en los artículos 8 y 17 de Ley 34/2002, de 11 de julio.

b.) Sobre la aplicación territorial de la Directiva 45/96/CE y la normativa nacional de protección de datos.

Respecto de la aplicación territorial de la norma (Directiva 45/96/CE), concluye la Sala de lo contencioso de la Audiencia Nacional, en línea con la Sentencia de 13 de mayo de 2014 del TJUE, que esa Directiva es aplicable al caso de autos, al considerar "que el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa "en el marco de las actividades" de dicho establecimiento si éste está destinado a "la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor" (apartado 55). Para llegar a dicha conclusión, parte la Sentencia de "que Google España se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. Además, al estar dotada de personalidad jurídica propia, es de este modo una filial de Google Inc. en territorio español, y, por lo tanto, un "establecimiento", en el sentido del artículo 4, apartado 1, letra a), de la Directiva 95/46 " (apartado 49).

Continúa recordando la Sala como, según el criterio del TJUE, " las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades" (apartado 56). Y que" la propia presentación de datos personales en una página de resultados de una búsqueda constituye un tratamiento de tales datos". Pues bien, toda vez que dicha presentación de resultados está acompañada, en la misma página, de la presentación de publicidad vinculada a

los términos de búsqueda, es obligado declarar que el tratamiento de datos personales controvertido se lleva a cabo en el marco de la actividad publicitaria y comercial del establecimiento del responsable del tratamiento en territorio de un Estado miembro, en el caso de autos en el territorio español (apartado 57)".

Por tal motivo, concluye la Sentencia de la Audiencia Nacional, en línea con la del TJUE, que la normativa europea en la materia, y también la legislación del país del Estado miembro de la Unión Europea en el que se encuentre el establecimiento (en este caso España), es aplicable, ya que "el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro" (apartado 60).

c.) Sobre la alegada falta de legitimación pasiva por parte de Google España.

Por la demandante Google España, S.L. se alegaba en la demanda la falta de legitimación pasiva de esa mercantil, al entender que "es un simple agente de Google Inc, dedicado a la promoción de la actividad publicitaria de Google" (en este caso en España), "no teniendo intervención alguna en el funcionamiento del buscador ni en el tratamiento de datos, y ni siquiera dispone de los medios técnicos que harían falta para ello". Expone que "los servidores que alojan las páginas web no pertenecen a Google, ni están bajo su control", al tratarse de "equipos de terceros ajenos a Google que pertenecen al responsable de la web de que se trate, o a la empresa a la que hayan contratado para el alojamiento de sus contenidos" siendo Google Inc., con domicilio en California (U.S.A.), la titular del servicio de buscador Google en

Internet, tanto desde el sitio web www.google.es como desde www.google.com y también explota el espacio publicitario que se genera en esas páginas web.

Google España planteó ante la Sala su falta de legitimación "ad causam" (su imposibilidad de formar parte en el proceso por motivo del imposible incumplimiento de las pretensiones ejercitadas en el procedimiento), y alegó la nulidad de la resolución recurrida al amparo de lo dispuesto en los artículos 62.1.c) y 62.1.e) de la Ley 30/1992, de 26 de noviembre, por haber sido dictada prescindiendo total y absolutamente del procedimiento legalmente establecido, y "ordena algo imposible de cumplir".

La Sentencia desecha estos argumentos en aplicación de lo establecido en la letra d) del artículo 2 de la Directiva 95/46/CE[171] y artículo 3.d) de la LOPD[172], que contienen las definiciones de "responsable del tratamiento" y concluye que Google España, S.L. sería responsable del mismo porque la búsqueda de datos se lleva a cabo en el marco del servicio de búsqueda de Google Inc, junto con el que Google España conformaría una unidad de negocio, resultando esta última imprescindible para el funcionamiento del motor de búsqueda, ya que de ésta depende su rentabilidad.

Argumenta la Sala que no sería lógico excluir a Google España, S.L. de cualquier responsabilidad en el tratamiento de los datos personales que lleva a cabo Google Inc, tras afirmar que este tratamiento se sujeta al Derecho europeo "precisamente por haberse llevado a cabo en el marco de las

[171] Según el cual el "responsable del tratamiento" es "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario".
[172] "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".

actividades de su establecimiento en España, del que es titular Google España, S.L., y más aún tras aceptar la relevancia de su participación en la actividad conjuntamente desempeñada por ambas, en relación con el funcionamiento del motor de búsqueda y el servicio que mediante el mismo se presta a los internautas, que conlleva el tratamiento de datos personales que nos ocupa". Concluye la Audiencia Nacional que, en caso contrario, se vería afectado negativamente el efecto útil de la Directiva 95/46/ CE y la protección directa y completa de las libertades y de los derechos fundamentales de las personas físicas, en particular el derecho a la intimidad, en lo que respecta al tratamiento de datos personales, que tiene por objeto garantizar.

También enfatiza la Sentencia que Google España, S.L. ha venido actuando "como si fuese responsable del tratamiento de datos, tanto en procedimientos de tutela de derechos seguidos ante la Agencia Española de Protección de Datos como en diversas intervenciones ante Tribunales Españoles", motivo por el cual no resultaría coherente alegar ahora esa ausencia de legitimación pasiva[173] en aplicación de la denominada doctrina de los actos propios.

Por tal motivo, la Sala concluye que Google España, S.L. también es responsable del tratamiento de datos, al constituir con Google Inc. una unidad material que reúne las características de un establecimiento de los referidos en el artículo 4.1.a) de la Directiva 95/46/CE.

[173] La Sala hace referencia a distintos procedimientos de tutela de derechos sobre cancelación de datos personales seguidos en la Agencia Española de Protección de Datos, en los que la reclamación se dirigió contra Google Spain, S.L. y ésta actuó como si fuera responsable del tratamiento: TD/00299/2007 (resolución de 9 de julio de 2007), TD/00463/2007 (resolución de 9 de julio de 2007), TD/00814/2007 (resolución de 7 de abril de 2008), TD/00387/2008 (resolución de 3 de septiembre de 2008),TD/00420/2008 (resolución de 29 de diciembre de 2008), TD/0444/2008 (resolución de 4 de noviembre de 2008), TD/00569/2008 (resolución de 24 de septiembre de 2008) y TD/00580/2008 (resolución de 29 de diciembre de 2008).

Y ello a pesar de que, otros tribunales, españoles y extranjeros, antes y después de la Sentencia del TJUE de 13 de mayo de 2014, hayan podido acoger esa excepción de falta de legitimación pasiva de Google España, S.L. (o de la filial de Google Inc. en otros países europeos), en reclamaciones relacionadas con el buscador Google, por considerar a Google Inc. único responsable del motor de búsqueda[174].

---

[174] Sobre la responsabilidad de los buscadores, ha recogido NIEVES BUISAN en su artículo "El derecho al olvido: el nuevo contenido de un derecho antiguo". Publicado en *El Cronista del Estado Democrático y de Derecho*, nº 46. Ed. Iustel., varias resoluciones de derecho comparado, en la que se reconoce la responsabilidad de los buscadores, citando varias resoluciones, como la de la sentencia de la Cour d' appel de Paris, Pôle 1,de 9 de diciembre de 2009, que condenó a Google por asociar la palabra estafa (arnaque) a la empresa Direct Energie, ordenando la supresión de las sugerencias a estafa propuestas por el software Google.
"El Italia, reviste importancia la sentencia de la Sección Cuarta Penal del Tribunal de Milán el 12 de abril de 2010, en la que se condena (penalmente) a tres directivos de Google por violar el derecho a la intimidad de un menor afectado por el síndrome de Down, mediante la difusión de un video que muestra el trato vejatorio infligido. Sentencia que contiene trascendentes conclusiones, cuales son: 1) Google Italy es la "mano operativa y comercial" de Google Inc. en Italia. 2) A través del sistema AD Words y del reconocimiento de palabras clave, Google Italy tiene la posibilidad de gestionar y organizar los datos contenidos en Google Video. 3) Google Italy trata los datos de esos videos y, en consecuencia, es responsable a efectos de la legislación sobre la privacy. 4) El beneficio perseguido esta unido a la interacción comercial y operativa existente entre Google Italy y Google Video mediante el sistema AD Words y palabras clave. 5º) Todo esto prueba "una clara aceptación consciente del riesgo concreto de la inserción y divulgación de datos y también, sobre todo, sensibles, que habrían debido ser objeto de particular tutela" y demuestra "el interés económico vinculado a esa aceptación del riesgo y la clara consciencia de este último".
Y sobre todo, en Alemania, es asimismo trascendente la sentencia del Tribunal Constitucional Federal de 2 de marzo de 2010, que declara la nulidad de los § 100 g) del Código Procesal Penal y 113 a) y b) de la Ley Federal de Telecomunicaciones, introducidos por la Ley de 21 de diciembre de 2007 para trasponer la Directiva 2006/24/CE sobre conservación de los datos asociados a las mismas. Preceptos que se consideran incompatibles con la Ley Fundamental de Bonn, por infringir su artículo 10.1 que protege el secreto de las comunicaciones y vulnerar el derecho a la autodeterminación informativa, por lo que se declaran nulos.
En la Jurisprudencia del propio Tribunal de Justicia de la Unión Europea (TJUE), encontramos también algún antecedente de interés. El primero de ellos es la sentencia del Pleno, de 6 de noviembre 2003, asunto C-101/2001 (Caso Lindqvist), que aunque no referida específicamente a los buscadores en Internet (en dicha fecha todavía no existían), declaró ya que hacer referencia, en una página Web, a datos de carácter personal, debía considerarse tratamiento de datos, de conformidad con el artículo 2.b) de la Directiva 95/46.
En la sentencia de 23 de marzo de 2010, asuntos acumulados C-236/08 a C-238/08 (Caso Louis Vuitton), dictada en materia de "marcas", el Tribunal de Justicia analiza la actividad de Google como motor de búsqueda, en su faceta de anunciante. Declara que el titular de una marca está facultado para prohibir a un anunciante que, a partir de una palabra clave idéntica a la marca, que haya seleccionado sin consentimiento del titular en Internet, haga publicidad de productos o servicios idénticos a aquellos para los que se ha registrado la marca, cuando dicha publicidad no permite o apenas permite al internauta medio determinar si los productos o servicios incluidos en el anuncio proceden del titular de la marca o si, por el contrario, proceden de tercero".

d.) Puntualizaciones formuladas en la Sentencia sobre el derecho a la protección de datos y libertades de expresión e información.

La Sentencia dedica su apartado duodécimo a delimitar el marco general de los derechos en conflicto en el supuesto objeto del procedimiento. Empleará los fundamentos de derecho siguientes a exponer los criterios de ponderación que debieran aplicarse en este tipo de conflictos (fundamento de derecho décimo tercero), y aplicarlos seguidamente al caso de autos (fundamento de derecho décimo cuarto).

En particular, y respecto de la colisión que se produce en el supuesto de autos entre la protección de datos de carácter personal y las libertades de información y expresión, subraya la Sentencia que el derecho a la protección de datos "es un derecho más amplio que el derecho fundamental a la intimidad personal y familiar", ya que el derecho fundamental a la protección de datos "amplía la protección constitucional a otros datos, sean o no íntimos, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, como aquéllos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad. También alcanza a aquellos datos personales públicos que, por el hecho de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos.

Respecto de ese derecho a la protección de datos de carácter personal sigue argumentando la Sentencia que "el derecho fundamental a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se

contienen en el derecho a la intimidad, con el objeto de garantizar a la persona un poder de control sobre sus datos personales" y que entre ellos "destacan el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. De este modo se garantiza el poder de disposición sobre los datos personales".

Sobre las libertades de información y expresión, recuerda que ambas constituyen derechos individuales que son derechos que "ostentan todas las personas físicas y que pueden ser ejercidos a través de la palabra, el escrito o cualquier otro medio de reproducción", "sin perjuicio de que cuando tales libertades son ejercidas por profesionales de la información a través de un vehículo institucionalizado de formación de la opinión pública, su grado de protección alcance su máximo nivel (STC 165/1987, de 27 de octubre)".

Incide la Sentencia en que el reconocimiento de la libertad de expresión "garantiza el desarrollo de una comunicación pública libre que permita la libre circulación de ideas y juicios de valor inherente al principio de legitimidad democrática". Mereciendo una protección constitucional reforzada aquellas ideas que coadyuven a la formación de la opinión pública libre, "faciliten que el ciudadano pueda formar libremente sus opiniones y participar de modo responsable en los asuntos públicos".

Tomando la anterior como punto de partida, recuerda la Audiencia en la Sentencia analizada que "al igual que sucede con los restantes derechos fundamentales", "el ejercicio del derecho a la libertad de expresión está sometido a límites que el Tribunal Constitucional ha ido perfilando progresivamente". De tal forma que, "no ampara la presencia de frases y expresiones injuriosas, ultrajantes y ofensivas sin relación con las ideas u opiniones que se expongan y, por tanto, innecesarias a este propósito, ni

protege la divulgación de hechos que no son sino simples rumores, invenciones o insinuaciones carentes de fundamento, ni tampoco reconoce un pretendido derecho al insulto".

También expresa que, con carácter general, la protección de los artículos del art. 18 CE se debilitará respecto de la de los del art. 20 CE, "si los asuntos tratados se ejercitan en conexión con asuntos que son de interés general, por las materias a que se refieren y por las personas que en ellos intervienen" y "contribuyan a la formación de la opinión pública", que es lo que sucede cuando afectan a personas que ejercitan funciones o cargos públicos, o "resultan implicadas en asuntos de relevancia pública", "obligadas por ello a soportar un cierto riesgo de que sus derechos subjetivos de la personalidad resulten afectados por opiniones o informaciones de interés general"[175].

e.) Los criterios de ponderación.

Al marco general de aplicación a los derechos en conflicto expuesto en el apartado precedente hay que sumar el contenido de la regulación específica de protección de datos vigente en el ordenamiento comunitario y nacional, y la interpretación que de esa norma hizo el TJUE en la aludida *Sentencia Google*.

En particular, subraya la Sentencia que el artículo 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de "si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre", sin que "la apreciación de la existencia de tal derecho presuponga que la inclusión

[175] SSTC 107/1988, de 8 de junio, 20/2002, de 28 de enero, 160/2003, de 15 de septiembre, 151/2004, de 20 de septiembre, y 9/2007, de 15 de enero.

de la información en cuestión en la lista de resultados cause un perjuicio al interesado". Y ello porque los artículos 7 y 8 de la Carta de derechos fundamentales de la UE "reconocen el derecho a solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados", y que estos derechos "prevalecen, en principio, no solo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona" salvo que la injerencia en sus derechos fundamentales esté justificada "por razones concretas, como el papel desempeñado por el interesado en la vida pública" o "por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate".

Se reproducen en la Sentencia los criterios contenidos en la del TJUE, con referencia a los párrafos de aplicación, y se señalan hasta diez criterios que han de considerarse en el caso objeto de controversia:

1) Estima que la interpretación de los criterios contenidos en la Directiva 45/94 y el análisis de los derechos en conflicto ha de hacerse partiendo de la amplia cobertura que esos derechos fundamentales otorgan a los interesados. En este caso se considera que los resultados que puede arrojar un motor de búsqueda en relación un individuo partiendo de su nombre y apellidos pueden constituir una injerencia grave en esos derechos fundamentales.

2) Todo tratamiento debe ser conforme a los principios de legitimación del tratamiento y calidad de datos contenidos en los artículos 6 y 7 de la Directiva. Esos principios de protección tienen reflejo tanto en las obligaciones que incumben a los responsables del tratamiento como en la

obligación de informar al interesado de que ese tratamiento se está llevando a cabo.

3) El responsable del tratamiento debe garantizar que los datos que no respondan a la exigencia de calidad sean suprimidos o eliminados, lo cual puede suceder tanto cuando los datos sean inexactos como cuando sean "inadecuados, impertinentes o excesivos" o que no estén actualizados, a menos que se imponga su conservación por fines históricos, estadísticos o científicos.

4) El interesado puede presentar una solicitud con base en el artículo 12.1.b) de la Directiva o ejercer el derecho de oposición que le ofrece el artículo 14 de ese mismo texto legal; en este segundo supuesto debe llevarse a cabo el balance entre los derechos en conflicto y, en el caso de entenderse justificada la reclamación, el responsable del tratamiento no podrá volver a referirse a esos datos.

5) El interesado ejercitará su derecho ante el responsable del tratamiento. Y si el responsable no atiende esa solicitud, podrá acudir, sea a la autoridad, sea a los Tribunales, para que se tutelen sus derechos.

6) "Un tratamiento inicialmente lícito de datos exactos puede devenir, con el tiempo, incompatible con la Directiva, cuando estos datos no sean necesarios en relación con los fines para los que se recogieron o trataron, en particular, cuando son inadecuados, no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido"[176].

7) Los derechos de la persona prevalecen con carácter general y salvo que, por razones concretas, exista un interés de la opinión pública de conocer

[176] Apartado 93 de la Sentencia del TJUE.

esos datos, justificado, por ejemplo, por el desempeño de un papel en la vida pública.

8) Ese equilibrio puede depender también de aspectos tales como "la naturaleza de la información", "el carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de la información", subrayándose asimismo que ese interés puede variar "en función del papel que esa persona desempeñe en la vida pública", siendo que en ese caso el órgano judicial quien deberá comprobar qué interés es preponderante, si el del reclamante o el del público.

9) También señala la sentencia que el resultado de esa ponderación puede ser distinto dependiendo de si lo hace el responsable del motor de búsqueda o el editor de una página web. En el criterio del TJUE, que ha recogido la AN en la Sentencia estudiada, es que el alcance potencialmente dañino de la inclusión de esa información en una lista de resultados es potencialmente mayor que su mantenimiento en una web determinada.

10) Ese derecho a que la información relativa a una persona sea desindexada no presupone que la misma cause un perjuicio al interesado.

En el apartado siguiente se procede a la aplicación de los criterios enumerados al caso objeto de controversia.

f.) Aplicación de los criterios de ponderación al caso.

En este punto, la Sentencia de la Audiencia Nacional es contundente y reproduce las conclusiones alcanzadas por el TJUE. En particular concluye que nos hallamos "ante un tratamiento de datos inicialmente lícito de datos exactos por parte del buscador Google que dado el tiempo trascurrido no son

necesarios en relación con los fines para los que se recogieron o trataron". Que en este caso "la libertad de información se encuentra satisfecha por su subsistencia en la fuente, es decir, en el sitio web donde se pública la información por el editor, sin que el hecho de eliminar de la lista de resultados los vínculos a las páginas web objeto de reclamación por el afectado, impida que utilizando otros datos se llegue a las citadas páginas web, pero no a partir de su nombre.

Y que por tanto el Sr. Costeja "tiene derecho a que la información sobre una subasta de inmuebles relacionada con un embargo derivado de deudas a la Seguridad Social ya no esté vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de sus datos personales".

g.) Interpretación de la resolución de la AEPD.

La Audiencia Nacional dedica su penúltimo fundamento de derecho (el decimoquinto), a aclarar la forma en la que debe interpretarse la parte dispositiva de la resolución recurrida. En palabras de la Sentencia esa redacción "no es afortunada", pues insta a que se "adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos", sin que sea claro que deben hacer exactamente los responsables del motor de búsqueda.

Para evitar las dudas interpretativas que podrían surgir sobre el alcance de las obligaciones asignadas a Google, la Sala determina que "la obligación impuesta por la resolución recurrida debe interpretarse en el sentido de que debe adoptar las medidas necesarias para retirar o eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre del reclamante, los vínculos a las páginas web objeto de reclamación".

Por todos los anteriores razonamientos, se desestima el recurso contencioso administrativo interpuesto por Google, y se confirma la adecuación a Derecho de la Resolución dictada por el Director de la Agencia Española de Protección de Datos.

3.3.2. La Sentencia de la Sección 6ª de la Sala de lo contencioso-administrativo del Tribunal Supremo, núm. 1611/2016 de 4 julio

No conforme con ello solo la entidad Google España, S.L. interpone recurso de casación contra dicha Sentencia, en el que se hacen valer cuatro motivos de casación, el primero articulado a través del artículo 88.1.c) de la LJCA (RCL 1998, 1741) y los otros tres con base en la letra d) de este mismo precepto.

El Tribunal Supremo estima haber lugar a ese recurso de casación en cuanto entiende debió estimarse el recurso contencioso-administrativo de Google España, manteniendo todos los pronunciamientos frente a Google Inc.

En particular, Google reprocha a la Sentencia de la Audiencia Nacional atribuir a Google España una corresponsabilidad en el tratamiento de datos personales objeto de recurso "con el argumento de que esta compañía y Google Inc. conforman una "unidad de negocio" o "unidad material", argumento este al que el Tribunal " a quo" añade la aplicación de la doctrina de los "actos propios" en el sentido de que Google España ha reconocido su condición de responsable del tratamiento al actuar como tal frente a terceros"[177].

[177] Fundamento de derecho cuarto, párrafo 2º.

La Sala estima los argumentos de Google España, en coherencia con resoluciones anteriores[178]. Entiende el Tribunal Supremo que, según la ley, es al responsable del tratamiento al que deben exigirse e imponerse las obligaciones derivadas del ejercicio del derecho al olvido y al que corresponde la adopción de las medidas oportunas para su cumplimiento.

En congruencia con lo anterior, argumenta:

- Que el procedimiento para el ejercicio de los derechos de oposición, acceso, rectificación y cancelación no se dirige ante Google España según la LOPD. Y ello porque esa LO establece que el ejercicio de tales derechos "deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, con el que se sigue el procedimiento correspondiente".

- Que en ese tratamiento no es posible la corresponsabilidad por parte de Google España, "en los términos que prescribe el nuevo Reglamento (UE) 2016/679 al regular precisamente esta figura de la corresponsabilidad en el tratamiento de datos", "estableciendo en el artículo 26 que, cuando dos o más responsables determinan conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables", éstos "determinarán de modo trasparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos de los interesados". En el criterio del Tribunal "difícilmente puede considerarse a Google España, S.L. responsable, ni tan siquiera corresponsable, del tratamiento controvertido, consistente, como se ha dicho, en hallar información publicada o puesta en

[178] Sentencias de 11 de marzo -recursos 643/2015 (RJ 2016, 1519) y 1482/2015 (RJ 2016, 1519), 14 de marzo -recursos 1078/2015 (RJ 2016, 1525) y 1380/2015 (RJ 2016,1071) y 15 de marzo de 2016 (RJ 2016, 1301)-recurso 804/2015- y las que les siguen, recursos de semejante contenido, cuyo criterio también se sigue en la presente sentencia.

Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, finalmente, ponerla a disposición de los internautas, cuando en dicha entidad no concurren ninguno de los dos elementos que definen tal condición", "pues no consta participación alguna de dicha sociedad en la gestión del motor de búsqueda y determinación de los fines y medios de dicho tratamiento", "ni existe asunción o atribución a la misma de responsabilidad en el cumplimiento de alguna de las obligaciones que la norma impone al responsable del tratamiento".

- Rechaza también el Tribunal Supremo que esa atribución de la condición de responsable del tratamiento a Google España. S.L. pueda ejercitarse "con base en la unidad de mercado -unidad material o funcional.- que conforma esta sociedad con Google Inc., con apoyo en los pronunciamientos del TJUE de 13 de mayo de 2014" "pues el propio Reglamento (UE) 2016/679 incluye entre las definiciones de su artículo 4 la correspondiente a "establecimiento principal", que en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, es el "lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones". El alcance de este concepto se explica en el considerando 36, según el cual, "el establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de las actividades de gestión que determinan las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables". "Se trata de un concepto de carácter funcional en cuanto supone el ejercicio y desempeño efectivo de las atribuciones determinantes del tratamiento de datos, fijación de los fines y medios". En estas circunstancias "resulta manifiesto, como se ha indicado, que en la entidad Google España, S.L. no concurren los requisitos y condiciones que permitan

considerarla como establecimiento principal del responsable (Google Inc.) en la Unión".

- Finalmente, concluye el Tribunal Supremo que "tampoco puede sustentarse el otro título de atribución de corresponsabilidad en el tratamiento de datos a Google España, S.L., que utiliza la Sala de instancia sobre la base de que esta entidad ha venido actuando como si fuese responsable del tratamiento de datos, tanto en procedimientos de tutela de derechos seguidos ante la Agencia Española de Protección de Datos como en diversas intervenciones ante Tribunales Españoles" en aplicación de la denominada "doctrina de los actos propios". Y ello porque "difícilmente puede atribuirse tal naturaleza de actos propios, a los efectos aquí examinados, a la participación de Google España en los procedimientos administrativos y procesos judiciales referidos en la sentencia de instancia cuando: en primer lugar, la propia Sala de instancia no habla de actuaciones indubitadas o concluyentes por parte de Google España, S.L., en el sentido de asumir la condición de responsable del tratamiento, sino que, por el contrario, dice que *estamos ante un indicio*"; segundo, porque "no se advierte ni valora por la Sala de instancia la distinta condición en que puede intervenir en tales procedimientos una persona"; tercero, porque "solo la comparecencia como responsable del tratamiento de datos, es decir, de la determinación de los fines y medios del tratamiento de datos, puede dar lugar a manifestaciones o actos válidos de reconocimiento de tal condición"; cuarto, "que la condición de responsable del tratamiento de datos viene definida legalmente, como se ha indicado antes de forma prolija, y su régimen jurídico no puede modificarse por las actuaciones de quien carece de facultades de disposición al respecto"; y quinto, "que la legitimación ha de examinarse en cada procedimiento y, por lo tanto, ha de estarse a la actitud del compareciente en el mismo, que este caso ha sido, desde la vía administrativa, negar tal legitimación".

Por todo ello, estima el recurso contencioso administrativo interpuesto por la entidad mercantil Google España, S.L. contra la Resolución de 30 de julio de 2010 dictada por el Director de la Agencia Española de Protección de Datos, que se anula en cuanto a la obligación impuesta a Google España, S.L., de adoptar las medidas necesarias para hacer efectivo el derecho de oposición ejercitado por el interesado en calidad del responsable del tratamiento de datos, debiendo mantenerse la resolución en cuanto impone esa misma obligación en concepto de responsable del tratamiento a la sociedad Google Inc.

El Tribunal Supremo acoge los argumentos de Google España en el exclusivo sentido de estimar su falta de legitimación pasiva y reenvía a los afectados por el tratamiento de sus datos personales a ejercitar sus derechos ante la matriz, Google Inc., con sede en California. Y ello en el entendimiento de que Google España no es responsable de ese tratamiento en los términos en que ese concepto es entendido por el nuevo Reglamento Europeo de Protección de Datos, ni puede concluirse tal cosa de otras actuaciones anteriores de la aludida compañía, ni tal conclusión puede extraerse tampoco del mero hecho de ser ambos una unidad de negocio. No obstante lo anterior, mantiene el resto de pronunciamientos de la Sentencia de instancia en relación con el reconocimiento del derecho al olvido.

En contraste con lo anterior, la Sala de lo civil del Tribunal Supremo si ha atribuido responsabilidad a Google España en asuntos de tutela de protección de datos.

En particular, cree esa Sala del TS que si es posible dirigirse en vía civil frente a Google España en procedimientos de tutela de derechos, ya que otra cosa haría prácticamente imposible su ejercicio, abocando a los interesados a procesos judiciales largos y costosos. En el criterio de la Sala de lo civil es posible ejercitar esos derechos frente a Google España ya que tiene consideración de "responsable" en nuestro país del tratamiento efectuado por Google en el sentido establecido por la Sentencia del TJUE de 2014.

Estas conclusiones han sido alcanzadas, por ejemplo, en la Sentencia núm. 210/2016 de 5 abril, del Pleno de la Sala de lo Civil del Tribunal Supremo, que confirma otra de la Audiencia provincial de Barcelona[179].

En esa resolución judicial, la Sala de lo civil del Tribunal Supremo descarta la exención de responsabilidad fallada en la jurisdicción contenciosa respecto de esa compañía, argumentando que "las sentencias de la Sala de lo Contencioso-Administrativo del Tribunal Supremo" "no resultan condicionantes o decisivas para resolverlo". Que "tales sentencias no tienen efecto prejudicial respecto de la resolución que haya de adoptarse en el presente recurso" recordando que es posible "la existencia de distintos criterios rectores en las distintas jurisdicciones, por la diversidad de las normativas que con carácter principal se aplican por unas y otras." Considerando en este caso que "en las sentencias de la Sala de lo Contencioso Administrativo se está resolviendo con relación a resoluciones dictadas en un procedimiento administrativo seguido ante la AEPD, mientras que esta sentencia se dicta en un proceso civil que tiene por objeto la protección de los derechos fundamentales del demandante, en concreto los derechos al honor, a la intimidad y a la protección frente al tratamiento automatizado de sus datos de carácter personal".

Y en este caso estima la Sala que Google España es responsable junto con Google Inc del tratamiento de estos datos personales, y que por tanto "está sometida a todas las obligaciones que se derivan de la Constitución, el Convenio Europeo de Derechos

[179] Sentencia de 17 de julio de 2014, dictada por la Audiencia Provincial de Barcelona (sección 16ª), en el rollo de apelación nº 99/2012, dimanante de los autos de juicio ordinario nº 411/2011 del Juzgado de primera instancia nº 8 de Barcelona.
En ese procedimiento, una persona solicitaba se declarase que se había producido una intromisión en sus derechos fundamentales al honor, intimidad personal y familiar y derecho a la protección de datos de carácter personal, por la indexación por distintos motores de búsqueda- Yahoo, Google, etc.-, bajo una búsqueda con su nombre y apellidos, de noticias vinculadas a una condena penal del año 1981 y posterior indulto en el año 1999.
La Audiencia rechazó, con base en la argumentación contenida en la Sentencia del TJUE, la alegación de falta de legitimación pasiva formulada por Google Spain y le condenó a indemnizar al actor con 8.000 €.

Humanos, la Carta de derechos fundamentales de la Unión Europea, el Convenio núm. 108 del Consejo de Europa de 28 de enero de 1981, la Directiva 1995/46/CE, de 24 octubre, del Parlamento Europeo y del Consejo de la Unión Europea, *de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* y la Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*, en la interpretación que de dichas normas han hecho tanto el Tribunal Constitucional y el Tribunal Supremo como el TJUE y el Tribunal Europeo de Derechos Humanos".

El Tribunal Supremo analiza el balance de los derechos en conflicto y estima, que aunque en un primer momento el interesado pudiera tener que soportar la publicación de sus datos en el BOE como beneficiario de un indulto y en cumplimiento de la legislación en la materia, en el presente caso la presencia de esos datos en Internet, mucho años después, supone una infracción del principio de calidad de los datos, por lo que Google debió haberlos retirado una vez fue requerido para ello por el interesado. Motivo por el cual desestima el recurso de Google y confirma la resolución de la Audiencia Provincial de Barcelona.

El Tribunal Supremo refrenda esta línea jurisprudencial a la que venimos de referirnos en el Auto de 4 de abril de 2018, por el que la Sala inadmite los recursos de casación y extraordinarios por infracción procesal frente a una Sentencia de la Audiencia provincial de Barcelona[180], que estimó la legitimación pasiva de Google frente a una reclamación por honor, intimidad y protección de datos de carácter personal, pero la desestimó en cuanto al fondo, resolviendo no había lugar a la retirada de los enlaces ni a la concesión de una indemnización, por ser el reclamante una persona con relevancia pública.

[180] Sentencia dictada con fecha de 29 de junio de 2017 por la Audiencia Provincial de Barcelona (Sección 11.ª), en el rollo de apelación n.º 259/2017 dimanante del juicio ordinario n.º 988/2015 del Juzgado de Primera Instancia n.º 22 de Barcelona.

3.3.3 Interrogantes sobre la aplicación de la Sentencia Google:

BUISÁN GARCÍA, , N. en el ya mencionado artículo *El Derecho al olvido: el nuevo contenido de un derecho antiguo*[181] pone de relieve algunas dudas prácticas que puede suscitar la aplicación de la *Sentencia Google*, y que entendemos interesantes destacar.

Por ejemplo, frente a la exigencia impuesta por el Tribunal de Justicia de la Unión Europea de que los resultados objeto de conflicto sean el resultado de una búsqueda "por el nombre y apellidos" del interesado; que el GT29 en sus directrices sobre la aplicación de esa Sentencia "amplió" al empleo de pseudónimos, diminutivos o nombres familiares que permitieran de la misma manera la identificación del afectado, BUISÁN plantea el escenario inverso, esto es, que en el buscador se introduzca o bien una palabra malsonante o insulto, o bien una conducta delictiva o reprobable, y que el nombre de una persona con nombre y apellidos apareciera en la lista de resultados arrojados por el buscador. En el mismo sentido, plantea la hipótesis de ser dos personas con los mismos nombres y apellidos, y que una de ellas plantee una reclamación por no venir los datos publicados referidos a ella. ¿Qué pasaría en una situación así? O si no será, al final, Google, quien decidirá qué resultados se muestran y cuáles no, sobre la base de editarlos.

Interrogantes a los que personalmente añadiría una reflexión sobre el alcance de la aplicación, o no, del derecho al olvido a una persona jurídica, y sobre si se terminará produciendo a futuro, o no, este reconocimiento, como sucedió en su momento con el reconocimiento del derecho fundamental al honor de las personas jurídicas.

Muchos son los interrogantes que se plantean en torno a este derecho nuevo y aun sin perfilar, pero de indudable relevancia en un mundo cada vez más conectado y digitalizado. Interrogantes que, no nos cabe duda, se irán resolviendo caso por caso y

[181] Publicado en *El Cronista del Estado Democrático y de Derecho*, nº 46. Ed. Iustel. (citado).

según los mismos se vayan planteando[182], al igual que sucedió en su momento en la interpretación que nuestros Tribunales vinieron haciendo en los supuestos de colisión de los derechos del art. 18 CE con los del art. 20 CE, hasta generar un prolijo cuerpo jurisprudencial que, con el paso del tiempo, ha ido dando respuesta pormenorizada al gran abanico se supuestos que se han venido sometiendo a su enjuiciamiento.

[182] Es ejemplo de lo anterior el dictado, por el propio TJUE de la Sentencia Manni, de 9 de marzo de 2017, en el asunto C-398/15. En ese asunto se resolvió por el Tribunal que, al amparo de las disposiciones de la Directiva 95/46/CE y de la Directiva 68/151/CEE (tendente a coordinar, para hacerlas equivalentes, las garantías exigidas en los Estados miembros a las sociedades mercantiles, para proteger los intereses de socios y terceros), corresponde a los Estados miembros determinar si las personas físicas "pueden solicitar a la autoridad responsable de la llevanza del registro central, del registro mercantil o del registro de sociedades, respectivamente, que compruebe, sobre la base de una apreciación caso por caso, si está excepcionalmente justificado, por razones preponderantes y legítimas relacionadas con su situación particular", "limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta de dichos datos".
http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=9111226

CAPÍTULO 4

LA RECEPCIÓN DE LA DOCTRINA DEL DERECHO AL OLVIDO POR LOS TRIBUNALES NACIONALES Y POR EL TRIBUNAL EUROPEO DE DERECHOS HUMANOS.

SUMARIO: 4.1. GENERAL; 4.2. COMENTARIO DE LA SENTENCIA DEL PLENO DE LA SALA DE LO CIVIL DEL TRIBUNAL SUPREMO DE 15 DE OCTUBRE DE 2015, DICTADA EN EL RECURSO DE CASACIÓN NÚM. 2772/2013, EN LA QUE SE ABORDA POR ESA SALA, POR PRIMERA VEZ, EL TRATAMIENTO QUE DEBE DARSE AL DENOMINADO "DERECHO AL OLVIDO DIGITAL" EN CASO DE CONFLICTO CON EL DERECHO A LA LIBERTAD DE INFORMACIÓN; 4.2.1. SUPUESTO DE HECHO; A) PROCEDIMIENTO SEGUIDO ANTE EL JUZGADO DE PRIMERA INSTANCIA Y PRONUNCIAMIENTOS CONTENIDOS EN LA SENTENCIA DEL JUZGADO DE PRIMERA INSTANCIA Nº 21 DE BARCELONA; B) EL RECURSO DEL MEDIO ANTE LA AUDIENCIA PROVINCIAL. DESESTIMACIÓN DEL RECURSO DE APELACIÓN E INTERPOSICIÓN DE RECURSO DE CASACIÓN; C) DECISIONES DEL PLENO DE LA SALA PRIMERA DEL TS SOBRE LOS MOTIVOS DE CASACIÓN PLANTEADOS; 4.2.2. ANÁLISIS DE LOS PRONUNCIAMIENTOS CONTENIDOS EN LA SENTENCIA DEL TRIBUNAL SUPREMO; 4.3. EL RECURSO DE AMPARO 2096/2016, FORMULADO FRENTE A LA SENTENCIA DEL TS QUE VENIMOS DE ANALIZAR: LA SENTENCIA DE LA SALA PRIMERA DEL TRIBUNAL CONSTITUCIONAL DE 4 DE JUNIO DE 2018; 4.4. CONCLUSIONES AL CONTENIDO DE LAS SENTENCIAS ANALIZADAS DEL TRIBUNAL SUPREMO Y CONSTITUCIONAL; 4.5. PRIMER PRONUNCIAMIENTO DEL TEDH SOBRE DERECHO AL OLVIDO DIGITAL: LA SENTENCIA DEL TEDH DE 28 DE JUNIO DE 2018, M.L Y W.W C/ ALEMANIA; 4.5.1 HECHOS Y PRONUNCIAMIENTOS DEL TRIBUNAL FEDERAL ALEMÁN; 4.5.2. FALLO DEL TEDH.

4.1. General

Ya hemos mencionado y es de sobra conocido para los lectores del presente trabajo que el apartado 4º del art. 18 de la Constitución Española establece que se limitará por ley "el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Precepto constitucional que consagra, pues, el derecho fundamental a la protección de datos, que se desarrolló a través de la aprobación, el 13 de diciembre del año 1999, de la Ley Orgánica 15/1999 (recientemente sustituida por la LO 3/2018), que tiene por objeto, según establece su artículo 1, "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las

personas físicas, y especialmente de su honor e intimidad personal y familiar". Por su parte, el art. 1º de la reciente LO 3/2018 establece como objeto de dicha norma: "la adaptación del ordenamiento español a los postulados del RGPD" y "la garantía de los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución".

No existen, en nuestro sistema constitucional, derechos absolutos, pero si una serie de derechos que actúan *como límite* sobre otros, habiéndose consolidado por una abundante doctrina y jurisprudencia los requisitos que deben cumplirse en el ejercicio de la libertad de información y expresión para poderlas considerar constitucionalmente legítimas y hacer prevalecer esos derechos sobre aquéllos del art. 18 CE[183][184], a saber, que la información difundida tenga relevancia pública y sea veraz, además de que la manifestación de la información se haga de forma correcta, empleando "expresiones y conceptos correctos, los que resulten necesarios para exponer las ideas", según exige nuestro Tribunal Constitucional desde la Sentencia del asunto Crespo Martínez, de 21 de enero de 1988[185][186].

Este planteamiento, originalmente aplicado a otros derechos del art. 18 CE (especialmente los consagrados en el apartado 1º de dicho artículo, honor, intimidad y propia imagen)[187], fue recogido y extendido al ámbito de la protección de datos por el Regulador español (la AEPD) hace ya más de una década (desde el año 2006[188]), al

183 Un resumen de esta jurisprudencia puede consultarse la obra de MUÑOZ MACHADO, S. *Los itinerarios de la libertad de palabra*, Ed. Crítica, Madrid 2013.
184 MUÑOZ MACHADO, S.: *Libertad de prensa y procesos por difamación*, Ariel, Barcelona, 1988
185 También MUÑOZ MACHADO, S., "Internet y los derechos fundamentales" *Anales de la Academia de ciencias morales y políticas* núm. 90, págs. 491 a 501.
186 Esta idea, aplicada al Derecho fundamental a la protección de datos de carácter personal la expone RALLO, A., en su obra *El Derecho al olvido en Internet: Google vs. España*, Ed. Centro de Estudios políticos y constitucionales, Madrid, 2015.
187 Asimismo, consultar el capítulo *"Comunicación Audiovisual y derecho al honor, intimidad e imagen"* de MUÑOZ-MACHADO CAÑAS, J. en el Tomo V. Audiovisual del Derecho de la Regulación Económica, dirigido por MUÑOZ MACHADO, S., Ed. Iustel. Madrid 2012.
188 Resolución de archivo de actuaciones de 24 de enero de 2006 en el expediente nº 27/2005: La reclamante alegaba que un determinado prestador el servicio de comunicación audiovisual había emitido en sus servicios informativos una noticia concerniente a un asesinato, mostrando una imagen

considerar que el derecho fundamental a la protección de datos del art. 18.4 de la CE, comparte con el derecho fundamental a la intimidad del art. 18.1 CE "el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, excluyendo del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"[189].

La Agencia Española de Protección de Datos, ya en Resolución de 24 de enero de 2006 (expediente nº 27/2005[190]), se pronunció a favor de las libertades informativas frente a la difusión de datos relativos a una determinada persona en el contexto de una investigación policial, argumentado que "de conformidad con la doctrina constitucional expuesta[191] y atendiendo a las circunstancias concurrentes en el (presente) supuesto, en relación a la relevancia pública de la información facilitada y a su veracidad, cabe entender que, resulta aplicable la doctrina legal de la posición preferente del derecho de expresión e información, frente al derecho a la protección de datos de carácter personal".

---

de un permiso de circulación con su imagen y sus datos. Dicha imagen, unida al hecho de que la denunciante estuvo domiciliada en la misma finca donde se produjo el asesinato, a juicio de la misma, le produjo "nefastas consecuencias" tanto para ella como para sus familiares. La AEDP privilegia el derecho a la libertad de opinión e información de la empresa editora del Informativo en el que apareció la noticia frente al derecho a la protección de datos de la denunciante, al entender que las informaciones difundidas serían en principio, acordes con las libertades de opinión e información, encuadradas en la denominación genérica de libertad de expresión, considerando muy especialmente que los datos de la denunciante asociados a una Licencia de Circulación, iban referidos a las pistas que investigaba la policía y no la relacionaban con el asesinato.

189 Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección1ª, de 24 octubre 2014.

190 V. Nota al pie nº 10.

191 Se citan expresamente en esa Resolución las Sentencias del TC 105/1983; 107/1988; 6/1988; 105/1990; 171/1990; 240/1992 y 204/1997, entendiendo que en las mismas el citado Tribunal "otorga una posición preferente a la libertad de expresión frente a otros derechos constitucionales, siempre y cuando los hechos comunicados se consideren de relevancia pública (Sentencias 105/1983 y 107/1988) y atendiendo a la veracidad de la información facilitada (Sentencias 6/1988, 105/1990 y 240/1992)".

En el mismo sentido se ha pronunciado la AEPD en otras resoluciones posteriores de fechas 4 de diciembre de 2006 (Expediente 847/2005); de 2 de marzo de 2007 (TD-00499-2006); de 26 de junio de 2007 (TD-00048-2007); de 23 de abril de 2007 (TD-00535-2006), entre muchas otras más; privilegiando en todas ellas las libertades de información y expresión sobre la tutela del derecho a la protección de datos de carácter personal, al entender prevalentes las primeras sobre el segundo cuando la información tiene relevancia para ser difundida y es veraz, y considerando de forma específica en el balance que ha de hacerse entre ambos derechos, el principio de proporcionalidad.

Este criterio general sobre la prevalencia de las libertades informativas sobre los derechos personalísimos del art. 18 CE, y en particular también respecto del derecho a la protección de datos de carácter personal, ha sido también refrendado por nuestros Tribunales, siendo paradigmática, por pionera en este ámbito, la aplicación formulada en la Sentencia de la Audiencia Nacional (de 25 de mayo de 2012; Fundamento Jurídico cuarto), según la cual:

> *"El ejercicio de la libertad de expresión y de información que amparaba al periódico implica el tratamiento de los datos personales de los sujetos objeto de la crítica y a la que se refiere la información, pues la utilización de los datos personales necesarios para el fin que se persigue y la libertad que se ejerce, se constituye un instrumento imprescindible sin el cual la crítica o la información carecería de sentido y se vaciaría de contenido. Es por ello que la utilización de los datos del denunciante estaba amparada por el ejercicio de la libertad de expresión e información sin que pueda utilizarse el derecho de cancelación para evitar la publicación de noticias o informaciones relacionadas con una o varias personas concretas, y si se considera que dichas noticias e informaciones vulneran su derecho al honor o son injuriosas o calumniosas son otras las vías que el ordenamiento jurídico ofrece para la defensa de sus derechos."*

Esto es, en el criterio de la Audiencia Nacional, y en aplicación de la jurisprudencia referida, cuando se difunden informaciones relativas a una determinada persona se manejan con necesidad datos personales (su nombre, su imagen), pero ese tratamiento debe entenderse amparado por el art. 20 CE y sin que frente al mismo puedan oponerse los derechos de cancelación u oposición regulados en la LOPD, al resultar en principio prevalentes los derechos del art. 20 CE sobre el derecho fundamental a la protección de datos de carácter personal (art. 18 CE). Cuestión distinta es si esas informaciones vulneran, o no, otros derechos fundamentales (honor, intimidad o imagen), aspectos que deberán dirimirse por las vías que el ordenamiento jurídico ofrece para la defensa de esos derechos (procedimientos tanto civiles como penales, según pudiera proceder).

En todo caso, al igual que sucede en la jurisprudencia en materia de derechos fundamentales al honor y a la intimidad personal y familiar, al realizar el balance que es preciso entre los derechos en conflicto, deben considerarse los principios generales y factores que ahora se recogen además, de forma expresa, en los considerandos cuarto (4[192]) y ciento cincuenta y cuatro (154[193]) del nuevo Reglamento europeo de

[192] (4) "El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística".

[193] (154) "El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la

protección de datos, a la luz de los cuales ha de aplicarse el art. 85 del RGPD, según los cuales ese tratamiento de datos personales "con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria" "debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta", lo cual debe aplicarse en particular "al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas", debiendo adoptarse medidas legislativas que establezcan "las exenciones y excepciones" "necesarias para equilibrar estos derechos fundamentales", siendo imprescindible que aborden aspectos tales como "los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos".

Esa excepción debiera haberse regulado de forma expresa por mandato específico del texto normativo comunitario, a través del texto de la LOPDDD (LO 3/2018), que es la nueva *Ley Orgánica de protección de datos de carácter personal y derechos digitales*, en vigor desde hace poco menos de un año.

Es preciso aludir también, en cuanto a la norma aplicable en la materia en los distintos Estados miembros de la UE se refiere, que establece asimismo el RGPD en el considerando 154 citado que en el supuesto de que las exenciones o excepciones

transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio".

difieran de un Estado miembro a otro, regirá el Derecho del Estado miembro que sea aplicable al responsable del tratamiento.

Finalmente, y en cuanto atañe a las colisiones entre el tratamiento de datos personales y los derechos fundamentales a la libertad de expresión e información[194], es preciso remitir también a la más reciente jurisprudencia y doctrina sobre el denominado "derecho al olvido digital"[195], que se aplica con más fuerza a los buscadores o motores de búsqueda en Internet, pero también a los medios de comunicación social[196], siendo esa doctrina de especial relevancia en cuanto se refiere al contenido de noticias en "archivos y hemerotecas", y sobre el que han tenido ocasión de pronunciarse recientemente nuestros Tribunales Supremo y Constitucional en un caso paradigmático que seguidamente se expondrá.

4.2. Comentario de la Sentencia del Pleno de la Sala de lo Civil del Tribunal Supremo de 15 de octubre de 2015[197]

El día 15 de octubre de 2015, el Pleno de la Sala primera del Tribunal Supremo dictó, por primera vez en nuestro país, una Sentencia referida al denominado "derecho al

194 BOIX PALOP, A.: "El equilibrio entre los derechos del artículo 18 de la Constitución, el "Derecho al olvido", y las libertades informáticas tras la Sentencia Google", *Revista General de Derecho Administrativo nº 38*. Ed. Iustel (2015).

195 Según la propia AEPD "El denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de Internet y hace referencia al derecho a impedir la difusión de información personal a través de Internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa". "En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)" (fuente: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php).

196 CASINO RUBIO, M.: "El periódico de ayer, el derecho al olvido en Internet y otras noticias". *Revista Española de Derecho Administrativo núm. 156*, Octubre-Diciembre de 2012, págs. 201 a 213.

197 Dictada en el Recurso de casación núm. 2772/2013, en la que se aborda por esa Sala, por primera vez, el tratamiento que debe darse al denominado "derecho al olvido digital" en caso de conflicto con el derecho a la libertad de información.

olvido digital"[198], entendido hasta el momento como la facultad de una persona de solicitar de un motor de búsqueda en Internet, la desindexación de entre los resultados que arroja la búsqueda por su nombre y apellidos de aquellas informaciones que, a pesar de haber sido exactas históricamente, han devenido imprecisas por el paso del tiempo, y cuya divulgación a día de la fecha afecta negativamente a su reputación[199].

4.2.1 Supuesto de hecho

Las dos personas demandantes (como así se alude a ellas en el texto de la Sentencia), habían resultado detenidas en los años ochenta por hechos relacionados con el tráfico de drogas. Al parecer, estas personas eran a su vez consumidoras de esas sustancias y, tras su detención, tuvieron que recibir asistencia médica por sufrir síndrome de abstinencia. Fueron condenadas en su día por estos hechos (delito de contrabando), pero posteriormente superaron su adicción a las drogas y desarrollaron normalmente su vida personal y familiar.

El periódico "El País" dio cuenta de esa noticia, aludiendo en su publicación tanto a la propia circunstancia de la detención, como a su motivo, el ingreso en prisión de los detenidos, la drogodependencia de sus protagonistas y el tratamiento médico recibido. Se incluían entre los datos que se ofrecían la identidad de esas personas tanto con su nombre y apellidos como con su profesión.

A pesar de que inicialmente la noticia se publicó únicamente en la versión papel del citado medio de comunicación social, con la puesta a disposición al público de forma gratuita en Internet de la hemeroteca del periódico "El País" en el año 2007 esa información quedó accesible al público, ya que no se había incluido en la misma

[198] GUICHOT, E.: "El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español", *Revista de Administración Pública*, 209, 45-92, ya citado.
[199] PAZOS-CASTRO, R.: "El derecho al olvido frente a los editores de hemerotecas digitales: A propósito de la STS (Pleno de la Sala 1ª) de 15 de octubre de 2015". *InDret*, Barcelona, octubre 2016.

ningún tipo de código ni instrucción informática (robots.txt o instrucción "noindex"), que técnicamente permiten su desindexación. Más aún, al parecer esas informaciones incluían las instrucciones "index" y "follow", que potenciaban su indexación y su inclusión en las bases de datos de los motores de búsqueda y mejoraban su posicionamiento en las listas de resultados obtenidos al realizar una búsqueda, de tal forma que cuando se realizaba una búsqueda con los nombres de los reclamantes en Google o Yahoo, el enlace a la hemeroteca digital de "El País" que contenía la noticia objeto de litigio aparecía en primera posición tanto en Google como en Yahoo en uno de los casos, y en primera posición en Google y en tercera en Yahoo, en el segundo supuesto.

En el año 2009, los demandantes solicitaron de la Editorial El País que "cesara en el tratamiento de sus datos personales en el sitio www.elpaís.com", sustituyendo sus nombres y apellidos por una mención genérica a sus iniciales, o que adoptara las medidas tecnológicas necesarias para que la página web de la noticia no fuera indexada por los motores de búsqueda en Internet. El País desatendió esa solicitud, al entender que esa publicación estaba amparada por el derecho a la libertad de información, ya que los hechos narrados eran ciertos y se contenían en la hemeroteca del medio, sin que pudiera procederse a su eliminación ni existían medidas que pudieran adoptarse para evitar que los proveedores de Internet indexaran a su vez la noticia.

a) Procedimiento seguido ante el Juzgado de Primera Instancia y pronunciamientos contenidos en la Sentencia del Juzgado de Primera Instancia nº 21 de Barcelona

En 2011 las personas demandantes promovieron demanda para la protección de sus derechos fundamentales al honor, intimidad personal y familiar y protección de datos de carácter personal (art. 18 CE), solicitando del Juzgado se declarase que se habían vulnerado tales derechos y solicitando se condenase a El País al cese de esa difusión,

adoptando las medidas que pudieran ser necesarias para que cesase el tratamiento de esos datos, o subsidiariamente, se sustituyese el nombre de los reclamantes por sus iniciales, obligando al medio a adoptar las medidas técnicas necesarias a fin de proceder a la desindexación de la información publicada de los referidos buscadores.

El Juzgado de Primera instancia (nº 21 de Barcelona, P.O. 1256/2011) estimó la demanda. Declaró que la difusión de la noticia constituía una intromisión en los derechos fundamentales al honor, intimidad personal y familiar y protección de datos de los demandantes por parte del medio, al que condenó al cese en la difusión de la noticia, a implantar las medidas tecnológicas adecuadas para impedir su difusión a futuro y evitar que la noticia apareciera en los buscadores de Internet al hacer búsquedas relacionadas con el nombre de los demandantes, introduciendo comandos "no index". También condenó al diario al pago a los reclamantes de una indemnización de 7.000 € a cada uno.

El Juzgado estimó que, a pesar de que la información pudiera haber sido veraz en su origen, el paso del tiempo y la posterior cancelación de los antecedentes penales de estas personas, hacía que la misma careciera actualmente de esa veracidad que es exigible para poder prevalecer frente al derecho al honor de los afectados, atentando contra su reputación y pudiendo lesionar su intimidad, estando la solicitud amparada en su derecho a la protección de datos de carácter personal.

b) El recurso del medio ante la Audiencia Provincial. Desestimación del recurso de apelación e interposición de recurso de casación

La Sentencia fue recurrida en apelación por el diario El País, alegando, de una parte, la caducidad de la acción y de otra, que la información era veraz en los términos exigibles jurisprudencialmente para entender prevalente frente a los derechos invocados el ejercicio de la libertad informativa.

Los demandantes se opusieron a dicho recurso e impugnaron la Sentencia de instancia, al entender que la misma había incurrido en incongruencia omisiva, al no haberse pronunciado sobre la necesidad de condenar al medio a suprimir sus nombres y apellidos del texto original de la publicación, o subsidiariamente, sustituirlos por iniciales tanto en la noticia como en el código fuente de la página web que la contiene. Asimismo, el Juzgado no se habría pronunciado sobre la necesidad de que en cualquier noticia que El País pudiera publicar sobre ese nuevo procedimiento, se omitieran los datos de los demandantes, para garantizar su anonimato.

La Sección 14ª de la Audiencia Provincial de Barcelona, en Sentencia de 11.10.2013 (rollo 486/2013), desestimó el recurso del medio y estimó la impugnación de los demandantes, añadiendo a la condena del diario El País dos medidas adicionales consistentes en la obligación de cesar en el uso de los datos personales de los reclamantes, "sin que puedan constar sus nombres y apellidos ni sus iniciales", estimando también la solicitud relativa a la prohibición de mencionar a los demandantes en posibles noticias sobre el presente procedimiento judicial.

Esa Sentencia fue recurrida en casación por el diario "El País", recurso que se fundamentaba en dos motivos diferenciados: 1) volvió a alegarse ante el TS la pretendida caducidad de la acción, ya que el contenido de la página web objeto del procedimiento sería el mismo que el de la noticia difundida en 1995, por lo que las alegaciones relativas a la falta de veracidad o interés público de la noticia se referirían

a una acción que estaría caducada (art. 9.5 de la LO 1/82) por el transcurso de más de cuatro años desde la publicación; y 2) infracción del art. 7 de la LO 1/82, de 5 de mayo, en relación con el art. 2.1 del mismo cuerpo normativo y en conexión con la vulneración del art. 20.1.d) de la CE.

Ese segundo motivo se fundamentaba, a su vez, en varias alegaciones diferenciadas: a) se critica por la recurrente que se le afee la finalidad económica perseguida con la digitalización de su hemeroteca, ya que ni el carácter privado del medio ni la utilización de publicidad como fuente de ingresos son circunstancias que impidan que su actuación esté amparada por la libertad de información; b) se alega que los hechos objeto de la noticia son veraces y tienen interés general, con independencia del transcurso del tiempo, ya que en la noticia consta su fecha de publicación, lo cual permite contextualizarla temporalmente; c) se argumenta asimismo que la expresión de los nombres y apellidos de los implicados en hechos delictivos está amparada por la libertad de información, según jurisprudencia constitucional; d) finalmente, se sostiene que el tratamiento de datos personales efectuado por "El País" sería un tratamiento de datos con fines periodísticos amparado en la libertad de información.

c) Decisiones del Pleno de la Sala Primera del TS sobre los motivos de casación planteados

La Sala alcanzó, en la Sentencia analizada, las siguientes decisiones sobre los motivos de casación planteados:

1º) Se desestima la alegada excepción de caducidad de la acción, ya que el objeto del procedimiento había quedado circunscrito, no a la noticia publicada en papel en los años ochenta, sino al "tratamiento de los datos personales" "consecuencia de la digitalización de la noticia con determinadas características técnicas que permiten su indexación y aparición en los resultados de los buscadores de Internet" vulnerando

los derechos al honor y a la intimidad de los demandantes, entendiendo la Sala que lo relevante para apreciar la caducidad de la acción no es cuándo se publicó la noticia en papel, sino si en el momento en el que se formula la demanda persiste el tratamiento de los datos personales que no cumple los requisitos y la normativa sobre protección de datos y causa un daño a los afectados, lo que sucedía en este caso.

2º) Circunscrito así el objeto del procedimiento, entiende la Sala que "ha de partirse de la licitud de la publicación de la información en la que aparecían las personas demandantes, y ceñir el enjuiciamiento al tratamiento de sus datos personales derivado de la digitalización de la hemeroteca del diario en que dicha información fue publicada".

La Sala, con cita a las Sentencias del TJCE dictadas en los asuntos Lindqvist (C-101/01, apartado 25[200]) y Google (C-131/12, párrafo 26), estima que el editor de una página web en la que se incluyen datos personales realiza un tratamiento de datos, y por tanto es responsable de que ese tratamiento cumpla las exigencias de la normativa que lo regula, y en particular las derivadas del principio de calidad de los datos (adecuación, pertinencia, exactitud y proporcionalidad). Por tal motivo, extiende las conclusiones alcanzadas por el Tribunal de Justicia de la Unión Europea en el asunto Google sobre las obligaciones de los gestores de motores de búsqueda a los editores de páginas web, considerando que los mismos son también responsables del tratamiento de datos, al serles técnicamente factible atender las solicitudes de desindexación mediante la introducción de comandos de exclusión (los mencionados robot.txt o códigos "noindex" "noarchive"), obligaciones que se derivan tanto de la propia Constitución como del Convenio Europeo de Derechos Humanos, de la Carta de derechos fundamentales de la Unión Europea, del Convenio núm. 108 del Consejo

[200]Sentencia del TJUE, *Lindqvist* (C-101/02);
http://curia.europa.eu/juris/document/document.jsf?text=&docid=50531&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=8120230

de Europa de 28 de enero de 1981, así como de la Directiva de protección de datos, la LO 15/1999, y la jurisprudencia que ha interpretado todas esas normas.

En el criterio de la Sala, los principios de adecuación, pertinencia, proporcionalidad y exactitud que conforman la calidad de los datos (art. 6 de la Directiva y 4 de la LOPD) deben analizarse considerando muy especialmente el "factor tiempo" ya que un tratamiento que "inicialmente pudo ser adecuado a la finalidad que lo justificaba" puede "devenir con el transcurso del tiempo inadecuado para esa finalidad", causando un daño desproporcionado en los derechos de la personalidad al honor y la intimidad.

Al efectuar el balance entre los derechos en conflicto en el supuesto de autos, el Tribunal Supremo considera preciso tener en cuenta los siguientes factores:

1º) Parte de la creencia, asentada en la jurisprudencia de esa Sala, de que el hecho de que la demandada sea una empresa de comunicación privada que, entre otros fines, busque el lucro comercial, no convierte *per se* su conducta en ilícita ni le priva de la protección derivada del ejercicio de las libertades de información y expresión reconocidas en el art. 20 CE.

2º) Argumenta que, a pesar de que las hemerotecas digitales entran en el ámbito de protección del art. 10 del CEDH por "suponer una importante contribución para la educación y la investigación histórica" al ser "fácilmente accesibles al público y generalmente gratuitos", su papel es "secundario" si se compara con el de la prensa escrita, y en consecuencia el ejercicio de la libertad de información es "menos intenso" que la propia publicación de noticias de actualidad.

3º) Considera asimismo para ponderar qué derechos deben prevalecer en el presente supuesto el carácter anónimo de los demandantes (quienes no son "personas con relevancia pública" entendiendo por tales a aquellas "personas que desempeñan un oficio público y/o desempeñan un oficio público y/o utilizan recursos públicos, y, en

un sentido más amplio, todos aquéllos que desempeñan un papel en la vida pública, ya sea en la política, en la economía, en el arte, en la esfera social, en el deporte o en cualquier otro campo" -Resolución 1165 de 1998, de la Asamblea Parlamentaria del Consejo de Europa sobre el derecho a la vida privada-) y el hecho de que "los hechos objeto de información carez[can] de interés histórico en tanto que vinculados a esas personas" (entendiendo que los sucesos delictivos son noticiables por su propia naturaleza, y con independencia de la condición de sujeto privado de la persona o personas afectadas por la noticia).

Valora muy especialmente la Sala que "en el caso objeto del recurso" los hechos hubieran tenido lugar "más de veinte años antes de que las personas demandantes hicieran uso frente a "El País" de su derecho de cancelación del tratamiento de sus datos", de tal forma que la "publicidad general y permanente de su implicación en aquéllos hechos" a través del indexado y archivo de los datos de esas personas en la hemeroteca de "El País" supone un daño desproporcionado en su honor (al vincularlas a hechos que afectaban seriamente su reputación) y a su intimidad (al hacer pública su drogodependencia en aquellas fechas). Incide la Sala en que "ciertamente eran hechos veraces" originalmente, pero subraya que habrían devenido inadecuados, impertinentes y excesivos con el paso del tiempo, vulnerando el principio de calidad de los datos anteriormente referido.

4º) Dispone algo que, en nuestro criterio, resulta clave en la presente resolución judicial, y es que "no puede exigirse al editor de la página web que por su propia iniciativa depure estos datos" porque ello supondría "un sacrificio desproporcionado para la libertad de información" a la vista de "las múltiples variables que debería tomar en consideración y de la ingente cantidad de información objeto de procesamiento y tratamiento en las hemerotecas digitales". Pero "si puede exigírsele que dé una respuesta adecuada a los afectados que ejerciten sus derechos de cancelación y oposición al tratamiento de datos y que cancele el tratamiento de sus datos personales cuando haya transcurrido un período de tiempo que haga inadecuado el tratamiento,

por carecer las personas afectadas de relevancia pública, y no tener interés histórico la vinculación de la información a sus datos personales".

Por tal motivo entiende que "la denegación por Ediciones El País de la cancelación del tratamiento de sus datos personales ante la solicitud hecha por las personas demandantes supuso una vulneración del derecho de protección de datos personales de las personas demandantes que trajo consigo la intromisión ilegítima en sus derechos al honor y a la intimidad".

5º) Entendiendo producida tal vulneración, la Sala analiza las medidas acordadas en la instancia, entendiendo pertinente y útil mantener la obligación impuesta al medio de "adoptar medidas tecnológicas" para que esa página no pueda ser indexada por los motores de búsqueda de Internet, ya que se entienden adecuadas para dar satisfacción al derecho de cancelación, en el criterio del Pleno del TS.

Sin embargo, las otras dos medidas impuestas en la Sentencia de la Audiencia Provincial de Barcelona [1.) eliminación de sus datos personas del código fuente de la página web que contiene la noticia, suprimiendo sus nombres y apellidos, y no permitiendo siquiera que consten sus iniciales; y 2) la adopción de medidas técnicas que eviten que la información pueda ser indexada por el propio buscador interno de "El País"] se revocan, ya que suponen, en el criterio del TS, "un sacrificio desproporcionado" y "censura retrospectiva" de informaciones que fueron "correctamente publicadas en su día", y una merma desproporcionada en la libertad de información protegida por el art. 20.1.d) de la Constitución.

Entiende la Sala que "hay una enorme diferencia entre la búsqueda de quien desee tener información específica pueda realizar acudiendo a las diversas hemerotecas, que el perfil completo que cualquiera pueda obtener en un buscador de Internet con tan solo introducir el nombre de una persona en Internet" entendiendo que "la supresión

de la primera posibilidad" "supone un daño desproporcionado para la libertad de información que ampara las hemerotecas digitales".

Por todo ello, estima parcialmente el recurso de casación del medio, manteniendo los pronunciamientos declarativos y los de condena, salvo en lo que se refiere a aquéllos relativos a la supresión de los datos personales de las personas demandantes en el código fuente de la página web que contenía la información y de su nombre y apellidos e incluso iniciales, y a la prohibición de indexar los datos personales para su uso por el motor de búsqueda interno de la hemeroteca digital, gestionada por la demandada, que se dejan sin efecto por los motivos ya dichos, y sin especial pronunciamiento sobre las costas en ninguna de las tres instancias.

4.2.2 *Análisis de los pronunciamientos contenidos en la Sentencia del Tribunal Supremo*

1. La Sentencia analizada tiene especial trascendencia a efectos jurisprudenciales por tratarse de la primera vez que la Sala de lo civil del TS (su Pleno) aplica a un asunto sometido a su enjuiciamiento la doctrina relativa al "derecho al olvido digital", integrando en un pronunciamiento jurisprudencial patrio del orden civil las soluciones alcanzadas en un supuesto muy similar sometido al enjuiciamiento del TJCE, a saber, el citado asunto Google c. España.

La Sentencia del TS emplea en el balance de los derechos en conflicto prácticamente los mismos parámetros que los utilizados en su momento por el TJCE en el asunto de GOOGLE, esto es: que el editor realiza un tratamiento de datos del que es responsable, debiendo garantizar la calidad de los datos tratados entendida como "adecuación, pertinencia, proporcionalidad y exactitud", siendo clave en el enjuiciamiento de ambos casos "el paso del tiempo" desde la publicación de la noticia original a la fecha actual y la circunstancia de que el responsable del tratamiento

recibió una solicitud de desindexación, que teniendo medios técnicos para atender, no estimó.

El derecho a la protección de datos del art. 18 CE se invoca en el supuesto analizado de forma indisolublemente vinculada a otros derechos consagrados en ese mismo art. 18 (honor e intimidad personal y familiar), siendo desde esa perspectiva del análisis del alcance y límites de ese derecho fundamental que se pronuncia por primera vez la Sala civil del TS y sobre las que hasta ese momento solo había tenido ocasión de pronunciarse la Sala de lo contencioso-administrativo, en aplicación de la función revisora de esa Sala respecto de las valoraciones realizadas por la AEPD.

Se acogen y reproducen por la Sala al realizar el balance de los derechos en conflicto, los argumentos contenidos en la aludida *Sentencia Google*, en la que se contemplan las hemerotecas como incluidas dentro del ámbito del art. 10 del CEDH, con un rol importante entre las labores de los medios de comunicación, pero "secundario" en relación con el desempeñado propiamente por la prensa escrita, considerando asimismo en el caso de autos el hecho de que ni las personas afectadas por las informaciones eran personajes públicos ni en los propios hechos informados tenía especial trascendencia la identidad de los reclamantes, sino la propia comisión en si misma del hecho delictivo.

Al igual que ocurrió al dictarse aquella Sentencia por el TJCE, sucede en el presente caso que el Tribunal deja claro que la ponderación ha de hacerse caso por caso, como se viene haciendo desde siempre en los conflictos entre los derechos del art. 18 CE con los del art. 20 CE, y sin poder instaurar de forma apriorística criterios universales que puedan aplicarse de forma general a todos los supuestos, aunque si sea posible sentar algún tipo de directriz o guía como las que el Grupo de trabajo del art. 29 ha procurado establecer para la aplicación de la *Sentencia Google*, y que de forma tácita han sido tenidas en consideración por al el TS en su pronunciamiento.

2. No obstante, existen dos diferencias importantes que deben destacarse entre el presente supuesto y el que le ha servido de antecedente y que son, en primer término, como el Tribunal Supremo emplea en la redacción de la Sentencia objeto de análisis especial celo en imposibilitar la identificación de las dos personas demandantes, omitiendo deliberadamente datos y fechas que pudieran permitir su reconocimiento, precisamente para respetar la finalidad buscada con el impulso de ese procedimiento judicial, que era proteger su privacidad y su anonimato.

No solo el Tribunal evita en todo momento mencionar a los recurrentes tanto en el encabezamiento de la Sentencia (aludiéndoles genéricamente como "A" y "B") como en el cuerpo y fallo de la misma, sino que se refiere a los mismos como "las dos personas demandantes", evitando en todo momento su identificación.

Si bien es cierto que no deja de ser una práctica común en la publicación de las Sentencias más recientes por el CENDOJ, sustituir los nombres y apellidos de las partes por otros ficticios o por sus iniciales, en el presente caso no es precisa dicha simulación, ya que la Sala ha optado por impedir esa identificación, *ab initio*, evitando mencionar a esas personas en todo momento.

Decisión que resulta especialmente llamativa si se compara con el pronunciamiento judicial que le ha servido de "antecedente" y que no es otro que la Sentencia del TJCE en el caso Google, en la que el reclamante de olvido, Sr. Costeja, será indefinida e irónicamente recordado precisamente por querer ser olvidado.

Sensible ante esa situación, el Pleno de la Sala Primera del TS se ha esforzado muy especialmente en evitar la identificación de las dos personas demandantes en el presente supuesto, esfuerzo que pudiera venir motivado, por la especial sensibilidad de los hechos que han dado origen a la posterior reclamación de olvido (tráfico y consumo de drogas), sensiblemente más graves que un embargo por una deuda a la Seguridad Social, que era el caso del Sr. Costeja, y la solicitud explícita en tal sentido

de los reclamantes en el presente asunto, que desde el inicio han solicitado que su identidad no trascendiera.

Posición de los demandantes que nos resulta coherente con la reclamación de intimidad que se formula, y que elogiamos, ya que resulta especialmente llamativo cuando encontramos supuestos (muy comunes) en los que los demandantes de intimidad solicitan la publicación de la Sentencia condenatoria en el mismo medio en el que se produjo la intromisión, u en otros de alcance equivalente.

Cabe sostenerse que, en los casos como el presente, la difusión de la Sentencia no debería estar nunca en el interés de los demandantes, ya que más que un efecto reparador, supondrían un recordatorio del daño sufrido. Las características propias de los derechos invocados hacen, en nuestro criterio, necesario matizar la aplicación de las disposiciones del art. 9.2 de la LO 1/1982, ya que, en general, la publicación de la Sentencia no contribuye a la reparación del daño, sino que, por el contrario, puede trasladar de nuevo a la opinión pública los hechos que se han considerado perjudiciales [en este sentido se han pronunciado las SSAP Madrid, Sec. 13ª núm. 83/2003, de 14 de noviembre; Sec. 19ª 193/1999 de 11 de marzo, y Sevilla, Sec. 6ª núm. 99/2004, de 23 de febrero].

3. La segunda diferencia que debe reseñarse es que la Sentencia del TS extiende la responsabilidad del encargado de la gestión de los motores de búsqueda a los editores de páginas web en la que se emplean datos personales, incidiendo especialmente en la posibilidad técnica que esos responsables tienen de desindexar las páginas objeto de controversia mediante la inclusión en sus cabeceras de los comandos informáticos adecuados.

La Sala modula acertadamente en esa resolución la responsabilidad de los responsables de los buscadores, entendiendo que esa responsabilidad no sería objetiva ni derivada de la mera digitalización del contenido, sino que exige se haya producido

por el afectado un requerimiento previo al medio, disponiendo expresamente que "no puede exigirse al editor de la página web que por su propia iniciativa depure estos datos" porque ello supondría "un sacrificio desproporcionado para la libertad de información" a la vista de "las múltiples variables que debería tomar en consideración y de la ingente cantidad de información objeto de procesamiento y tratamiento en las hemerotecas digitales". Y que lo que "si puede exigírsele" es que "dé una respuesta adecuada a los afectados que ejerciten sus derechos de cancelación y oposición al tratamiento de datos y que cancele el tratamiento de sus datos personales cuando haya transcurrido un período de tiempo que haga inadecuado el tratamiento, por carecer las personas afectadas de relevancia pública, y no tener interés histórico la vinculación de la información a sus datos personales".

Por ello, en este caso la condena del Tribunal Supremo viene motivada específicamente por "la denegación por Ediciones El País de la cancelación del tratamiento de sus datos personales ante la solicitud hecha por las personas demandantes" que se entiende supuso "una vulneración del derecho de protección de datos personales de las personas demandantes que trajo consigo la intromisión ilegítima en sus derechos al honor y a la intimidad".

4. Las conclusiones alcanzadas por el Tribunal Supremo no parecen desacertadas ni alejadas de las previamente establecidas por el TJCE en la *Sentencia Google*, si bien se plantea, como sucedió al dictarse aquella sentencia, el interrogante de cómo se aplicará esa jurisprudencia a cada uno de los supuestos diferenciados que puedan darse en el futuro, pudiendo establecerse de antemano unas directrices generales o guías de aplicación, pero debiendo realizarse dicho análisis, como se ha venido haciendo hasta la fecha en la colisión de los derechos del art. 18 con los del 20 CE[201], caso por caso[202].

[201] GRIMALT SERVERA, P.: *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, Ed. Iustel, Madrid 2007.
[202] CAVANILLAS MÚGICA, S. y GRIMALT SERVERA, P.: "Honor, intimidad y propia imagen", *Base de conocimiento jurídico*, Ed. IUSTEL.

Esta obligación, nos permite prever que se consolidará, a futuro, un cuerpo jurisprudencial específico en relación con los conflictos que afecten a estos dos derechos, y más particularmente, el derecho a la protección de datos de carácter personal, estrechamente vinculado a los derechos fundamentales de la persona, con los del art. 20 CE, lo que a su vez supondrá una inversión importante para el medio, que se verá obligado a establecer un cuerpo de vigilancia del cumplimiento de este tipo de reclamaciones, y muy previsiblemente criterios dispares sobre si esas solicitudes de rectificación deben o no ser atendidas.

5. Lo cual nos lleva a preguntarnos, como ya hemos apuntado anteriormente, qué organismo será el que vaya desarrollando ese cuerpo jurisprudencial y cómo se articularán la relación entre las distintas secciones del TS (civil y contenciosa), que deberán además conjugarse con las labores de la AEPD.

6. La LOPD, en su art. 19 y bajo la rúbrica, "derecho de indemnización" dispone que "los interesados que" "como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento" "sufran daño o lesión en sus bienes o derechos" "tendrán derecho a ser indemnizados", y que "en el caso de los ficheros de titularidad privada", "la acción se ejercitará ante los órganos de la jurisdicción ordinaria", lo cual ha sucedido en el presente caso y sin necesidad de que la realidad de los incumplimientos deba ser constatada previamente a través de sistema de tutela de derechos que establece la propia ley (art. 18 LOPD).

El TS se limita a confirmar en la resolución por la que resuelve el recurso de casación la pertinencia de la indemnización concedida en la instancia y su importe, por vulneración de los derechos consagrados en el art. 18 CE, infiriéndose respecto de la cuantía de esa indemnización del suplico de la demanda (transcrito en el antecedente de hecho primero de la Sentencia), que la solicitud de indemnización se formula a la luz de los parámetros del apartado 3º del art. 9 de la LO 1/1982, debiendo presumirse que son esos (y no otros), los criterios empleados por los Juzgadores de las Instancias

inferiores para la fijación del importe de la indemnización concedida (7.000 € a cada una de las dos personas demandantes).

Para la fijación del importe de esa cuantía indemnizatoria[203], el Tribunal Supremo ha aplicado los mismos parámetros que han venido utilizándose tradicionalmente para resarcir los daños producidos por los incumplimientos denunciados de los preceptos de la LO 1/1982, y para los que "la existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima".

4.3 El recurso de amparo 2096/2016, formulado por los recurrentes frente a la Sentencia del Tribunal Supremo que venimos de analizar: la Sentencia de la Sala primera del Tribunal Constitucional, de 4 de junio de 2018

Frente a la aludida Sentencia del Tribunal Supremo, se interpuso por los reclamantes incidente de nulidad de actuaciones, y posteriormente recurso de amparo, seguido con el núm. 2096-2016 ante la Sala Primera del Tribunal Constitucional.

Las personas recurrentes sostuvieron que tanto la Sentencia del Tribunal Supremo que hemos analizado como su providencia de 17 de febrero de 2016 vulneraban sus derechos al honor y a la intimidad personal y familiar, consagrados en el art. 18 de la Constitución Española, y ello porque a pesar de que la Sentencia reconocía la existencia de una vulneración en esos derechos, había moderado las medidas correctoras impuestas por la Audiencia provincial, resultando las mismas idóneas, en el criterio de los recurrentes.

[203] GARROTE FERNÁNDEZ-DÍEZ, I., "Indemnización por daños morales derivados de la publicación de resultados de buscadores que afectan al derecho al honor e intimidad y a la protección de datos personales", *Revista de Propiedad Intelectual*, núm. 54, 2016, págs. 13-66; ya citada.

En particular, se sostenían tres argumentos:

> 1) el primero, que debía mantenerse la obligatoriedad de eliminar sus nombres de la noticia, ya que a pesar de haberse desindexado en unos concretos buscadores, esto no obstaba para que, en el futuro, pudieran crearse otros que permitieran acceder a la información desindexada, imponiéndoles una "carga irrazonable" para la defensa de sus derechos;
>
> 2) el segundo, que "al anular las medidas tuitivas acordadas en apelación", las resoluciones recurridas habrían vulnerado el derecho fundamental a la protección de datos de los reclamantes (art. 18.4 CE), "al impedir el poder de disposición individual de un titular sobre sus propios datos".
>
> 3) En tercer y último lugar, se alegaba que las resoluciones recurridas vulneraban el principio de proporcionalidad por falta de motivación, y consecuentemente el derecho fundamental a la tutela judicial efectiva (art. 24.1 CE), al hacer prevalecer el derecho fundamental a la información y el "interés público que subyace" en ese derecho, "sin expresar" "la valoración sobre la idoneidad, necesidad y proporcionalidad en sentido estricto de las medidas solicitadas, que el mencionado juicio conlleva"[204].

Mediante providencia de 28 de noviembre de 2016, la Sala Primera del Tribunal Constitucional resolvió admitir a trámite el recurso de amparo, entendiendo que concurriría "especial transcendencia constitucional" (art. 50.1 LOTC), porque el recurso plantearía "un problema que afecta a un derecho fundamental" sobre el que no habría aún doctrina del Tribunal Constitucional.

[204] STC 58/2018, de 4 de junio de 2018, antecedente 3. Párrafo 5º.

El Ministerio fiscal ciñó el objeto del debate al enjuiciamiento, en el especial contexto de las hemerotecas digitales, a determinar si la prohibición de indexar los datos personales de los demandantes -nombre, apellidos e iniciales-, para su uso por el motor de búsqueda interno y la supresión de tales datos en el código fuente de la página web de EL PAÍS que contenía la información, eran medidas necesarias y proporcionadas para proteger los derechos fundamentales a la intimidad, honor (art. 18.1 CE) y a la protección de datos (art. 18.4 CE), o por el contrario, suponían una injerencia excesiva y desproporcionada en el derecho a la libertad de información del diario.

En la aludida Sentencia[205], el TC configura, por vez primera, el "derecho al olvido digital" en nuestra jurisprudencia constitucional, y de la siguiente forma:

> *"el derecho a obtener, sin dilación indebida, del responsable del tratamiento de los datos personales relativos a una persona, la supresión de esos datos, cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados; cuando se retire el consentimiento en que se basó el tratamiento; cuando la persona interesada se oponga al tratamiento; cuando los datos se hayan tratado de forma ilícita; cuando se daba dar cumplimiento a una obligación legal establecida en el Derecho de la Unión o de los Estados miembros; o cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de información".*

Continúa especificando esa Sentencia que:

> *"en el Reglamento (UE) 2016/679, del Parlamento y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en los que respecta al tratamiento de datos personales y a la libre circulación de estos datos[206]" "se viene a legislar de forma más clara*

[205] Sentencia de la Sala Primera del Tribunal Constitucional, de 4 de junio de 2018. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-9534
[206] https://boe.es/doue/2016/119/L00001-00088.pdf

> *el derecho a la protección de datos personales de una determinada base que los contuviera" existente ya en la Directiva 95/46/CE, "estrechamente vinculado a la salvaguarda del derecho fundamental a la protección de datos personales frente al uso de la informática (art. 18.4 CE), y con la proyección del art. 8 de la Carta de los derechos fundamentales de la Unión Europea y del Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecta al tratamiento automatizado de datos de carácter personal".*

En la Sentencia analizada, ese Alto Tribunal, define por primera vez en la jurisprudencia constitucional el derecho al olvido como "una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4 CE)", y como "mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo".

Con cita a la STC 292/2000, el TC recuerda la vinculación entre los párrafos 1º y 4º del art. 18 de la CE y subraya como el segundo:

> *"garantiza un ámbito de protección específico pero también más idóneo que el que podían ofrecer, por si mismos, los derechos fundamentales mencionados en el apartado 1 del precepto [art. 18 CE]" de modo que "la garantía de la vida privada de la persona y su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data), y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención" (STC 292/2000, FJ5 y jurisprudencia allí citada)".*

Dispone el TC respecto del derecho al olvido digital que: "si las libertades informáticas pueden definirse como derecho fundamental, también lo es, porque se

integra en ellas, el derecho al olvido". Conclusión que "puede extraerse sin dificultad de la configuración que hace nuestra jurisprudencia del art. 18.4 CE, al definirlo como un conjunto de derechos que el ciudadano puede ejercer "frente a quienes sean titulares, públicos o privados, de ficheros de datos personales" (STC 290/2000, FJ 7), y "establecer que tales derechos son, entendidos como haz de facultades de su titular, el derecho a consentir la recogida y el uso de sus datos personales y a conocer los mismos, el derecho a ser informado de quién posee sus datos personales y con que finalidad, y el derecho a oponerse a esa posesión y uso, exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos, esto es, el derecho de supresión (en este sentido, STC 290/2000, FJ7)".

En el criterio de Tribunal Constitucional, el reconocimiento del derecho al olvido como derecho fundamental, supone la aplicación al mismo, de forma automática, de la jurisprudencia relativa a los límites de los derechos fundamentales, según la cual éstos están limitados "por los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos" "pues así lo exige nuestra constitución" [207].

Partiendo de este planteamiento general, el TC analiza, en el concreto supuesto sometido a enjuiciamiento, la colisión producida en el caso frente el derecho a la autodeterminación sobre los propios datos personales y del derecho a la libertad de información, consagrada en el art. 20.1.d de la CE.

Analiza el TC la base fáctica de la Sentencia: el hecho de que la noticia en la que se contienen los datos personales de los reclamantes, que han solicitado su supresión, están contenidos en una noticia digitalizada, incluida a su vez en una hemeroteca digital, narrándose en esa noticia hechos ocurridos en los años 80 del siglo XX consistentes en la detención de los reclamantes en el contexto de una operación

[207] STC 290/2000, FJ 7

antidroga, su ingreso en prisión y necesidad de ser atendidas por padecer síndrome de abstinencia.

En tanto que exposición objetiva y fáctica de datos relativos a esa operación policial, la información detallada se incardinaría en el derecho del medio a comunicar libremente información veraz (art. 20.1.d CE), que "protege la difusión de hechos que merecer ser considerados noticiables por venir referidos a asuntos de relevancia pública que son de interés general por las materias a que se refieren o por las personas que en ellos intervienen"[208].

Digitalizada la noticia e incluida en la hemeroteca digital de EL PAÍS, fue enlazada en motores de búsqueda, ya que no se incluyeron protocolos de desindexación que permitieran excluir la información de esas búsquedas.

Los órganos judiciales de primera y segunda instancia que conocieron del asunto, fallaron a favor de los demandantes y de la desindexación de la noticia de los motores de búsqueda. Obligación no contestada por el Tribunal Supremo. Habiéndose revocado por ese Tribunal únicamente la obligación impuesta al medio en las instancias inferiores de ocultar los nombres de los reclamantes, sustituyéndolos por iniciales en el momento de incluir la noticia en la hemeroteca digital de EL PAÍS, tratándose, por tanto, de discernir si es legítimo o no emplear los nombres propios como criterio de búsqueda y localización de noticias en el entorno de una hemeroteca digitalizada. Expone acertadamente la Sentencia analizada que "en este contexto, los derechos que colisionan son, de un lado, el derecho a la supresión de datos de una base informatizada (art. 18.4 CE), en relación mediata e instrumental con la garantía del derecho al honor y la intimidad de las personas a las que conciernen los datos (art. 18.1 CE) y las libertades informativas del art. 20.1.d) CE".

[208] STC 41/2011, de 11 de abril, FJ 2

En el criterio del TC, en un conflicto como el presente deben emplearse los criterios que jurisprudencialmente han venido empleándose con normalidad para dirimir el balance entre los derechos en conflicto (derechos a la información versus derechos de la personalidad), doctrina coincidente además en lo sustancial con la del Tribunal Europeo de Derechos Humanos al interpretar el artículo 10 de la CEDH[209]. Pero debiendo adicionarse a esas variables otras dos de aplicación en asuntos como el que analizamos, en los que haya de dirimirse un conflicto en el que están involucrados los derechos del apartado 4º del artículo 18 de la CE, a saber: "el paso del tiempo a la hora de calibrar el impacto de la difusión de una noticia sobre el derecho a la intimidad del titular de dicho derecho" y "la importancia de la digitalización de los documentos informativos para facilitar la democratización del acceso a la información de todos los usuarios de Internet".

Recuerda esa Sentencia los requisitos que tradicionalmente ha exigido nuestra jurisprudencia para entender prevalentes los derechos a la libre expresión e información frente a los derechos protegidos por el art. 18 CE: 1) que la información difundida sea veraz (entendiendo esa veracidad, no como una exigencia de concordancia plena entre lo narrado y lo sucedido realmente, sino como la búsqueda diligente de esa verdad por parte de los profesionales de la información[210]), y 2) que tenga relevancia pública, en el sentido de considerar los mismos "noticiables" (lo cual puede suceder por el carácter noticioso de los hechos sucedidos, o porque los mismos vengan referidos a personas con relevancia pública).

Respecto de ese carácter noticiable, el TC puntualiza que ese carácter "también puede tener que ver con la actualidad de la noticia" entendida como "su conexión, más o menos inmediata, con el tiempo presente". Matizando que "la materia u objeto de una noticia puede ser relevante en el sentido abstracto, pero si se refiere a un hecho

[209] Con cita, en esa Sentencia a: SSTC 138/1996, de 16 de septiembre, FJ3; 144/1998, de 30 de julio, FJ2; 21/2000, de 31 de enero, FJ4; 112/2000, de 5 de mayo, FJ6; 76/2002, de 8 de abril, FJ3; 61/2004, de 19 de abril.
[210] Cita la STC 129/2009, de 1 de junio, FJ2.

sucedido hace diez años, sin ninguna conexión con un hecho actual, puede haber perdido parte de su interés público o de su interés informativo para adquirir, o no, un interés histórico, estadístico o científico". Subraya seguidamente la sentencia que este tipo de intereses "no guarda una relación directa con la formación de una opinión pública informada, libre y plural", sino con el desarrollo de general de la cultura, que "actúa como sustrato de la construcción de opiniones". En el criterio del Tribunal Supremo, "pasado un lapso de tiempo", podría ponerse en duda la prevalencia del derecho a la información frente al derecho fundamental a la intimidad, y que el trascurso del tiempo haga que datos que "pudieron tener relevancia pública en su día", deban ahora ser olvidados.

El Tribunal Constitucional entiende que "la universalización de acceso a las hemerotecas" "facilitado por su digitalización" "tiene un efecto expansivo sobre la capacidad de los medios de comunicación para garantizar la formación de una opinión pública libre" y que ese efecto expansivo "también supone un incremento del Impacto sobre los derechos fundamentales de las personas que protagonizan las noticias incluidas en las hemerotecas". Dependiendo el equilibrio de los derechos en conflicto de aspectos tales como "la naturaleza de la información de que se trate" de su carácter más o menos sensible para la vida privada de las personas afectadas y del interés público -o no- de disponer de esta información, que puede variar en función del papel que esta persona desempeñe en la vida pública.

Por todo lo expuesto en el presente epígrafe, el Tribunal Constitucional acuerda estimar parcialmente el recurso, teniendo en cuenta las circunstancias particulares del presente supuesto concreto, y específicamente:

- Que a pesar de resultar veraces los hechos relatados en la noticia frente a la cual pretende ejercitarse el "derecho al olvido", los mismos sucedieron en el marco de una investigación policial sucedida en los años ochenta, de tal modo que, la relevancia pública de la noticia, que en su momento no era discutible,

si lo es en el presente momento temporal, y al ser traída la misma al presente a través de medios digitales.

- Considera asimismo ese Tribunal, de forma muy especial, que las personas recurrentes ni eran personajes públicos en el momento de producirse los hechos ni lo son tampoco en el momento del dictado de la Sentencia.

- También considera en el balance de los derechos en conflicto que los datos revelados inciden muy directamente en el honor y la intimidad de los recurrentes, y que los hechos relatados sucedieron en el pasado, sin ninguna incidencia en el presente.

Concluye la Sala que los hechos relatados "carecen hoy día de toda relevancia para la opinión pública libre", más allá de los derivados de la pura publicación en una hemeroteca digital, por cuanto no son hechos actuales, ni de nueva noticia, ni contribuyen al debate público, siendo además los participantes en los hechos personas privadas, que si bien participaron en un suceso penal -en si mismo relevante- tampoco fue "particularmente grave ni ocasionó especial impacto en la sociedad de la época". Motivos todos ellos por los que "el transcurso de tan amplio margen de tiempo ha provocado que el inicial interés que el asunto suscitó haya desaparecido por completo", y que a la inversa, "el daño que la difusión actual de la noticia produce en los derechos al honor, intimidad y protección de datos personales de las personas recurrentes reviste especial gravedad, por el fuerte descrédito que en su vida personal y familiar origina la naturaleza de los datos difundidos". Así, el Tribunal entiende desproporcionado el daño que el mantenimiento de los datos de los recurrentes en la hemeroteca les suscita, ordenando se prohíba al medio (El País) indexar datos personales (nombre y apellidos de los recurrentes y su uso en el motor de búsqueda de El País), entendiendo que la aludida medida es "idónea, necesaria y proporcionada" a fin de evitar una difusión de la noticia lesiva de los derechos invocados. Entiende el Tribunal que "la medida requerida es necesaria porque su adopción, y solo ella,

limitará la búsqueda y localización de la noticia en la hemeroteca digital sobre la base de datos personales inequívocamente identificativos de las personas recurrentes" y a este respecto entiende que esa función puede quedar garantizada a través de otros parámetros (temáticos, temporales, geográficos o de cualquier otro tipo), sin perjuicio de que se suprima la posibilidad de efectuar la búsqueda acudiendo al nombre y apellidos de la persona en cuestión.

Entiende el TC que las personas integrantes de aquello que el TS califica de "audiencia más activa", puede acceder a la noticia por otros cauces, sin perjuicio de que se impida hacer un seguimiento "ad personam" del pasado de un determinado individuo, en este caso sin relevancia pública, entendiendo que las hemerotecas son herramientas dirigidas a garantizar la formación de una opinión pública plural, y "no a satisfacer la curiosidad individual y focalizada".

Asimismo, concluye la Sala que esa desindexación es bastante para conseguir el fin perseguido, y ello sin necesidad de la total "anonimizacion" de los recurrentes, y sin que sea necesaria ni la supresión del nombre y apellidos, ni la sustitución de éstos por sus iniciales en el código fuente de la página web que contiene la información. Estimando por ello (solo parcialmente) el recurso de amparo.

4.4 Conclusiones al contenido de las Sentencias analizadas del Tribunal Supremo y Constitucional

Los pronunciamientos contenidos en las Sentencias del Tribunal Constitucional y Supremo no parecen desacertadas ni alejadas de las previamente establecidas por el TJCE en la *Sentencia Google*, si bien se plantea, al igual que sucedió al dictarse aquella sentencia, el interrogante de cómo se aplicará esa jurisprudencia a cada uno de los supuestos diferenciados que puedan darse en el futuro, pudiendo establecerse de antemano unas directrices generales o guías de aplicación generales, pero debiendo

realizarse dicho análisis, como se ha venido haciendo hasta la fecha en la colisión de los derechos del art. 18 con los del 20 CE, caso por caso.

Esta obligación de analizar las colisiones entre los derechos del art. 20 y 18 de la CE caso por caso, nos permite prever que se consolidará, a futuro, un cuerpo jurisprudencial específico en relación con los conflictos que afecten al derecho a la protección de datos de carácter personal y los del art. 20 CE, similar al que existe ya en caso de colisión de las libertades de información y expresión y los derechos fundamentales al honor, intimidad personal y familiar y propia imagen.

Esa necesidad de valorar caso por caso los derechos en conflicto supondrá además, y al margen del cuerpo jurisprudencial que previsiblemente se desarrollará, una inversión importante para los medios de comunicación social (prensa escrita, audiovisual e Internet) en relación con la atención a este tipo de reclamaciones, viéndose obligados a establecer un cuerpo de vigilancia que compruebe cuando este tipo de reclamaciones son o no atendibles, pudiendo ser interesante, en la medida de lo posible, coordinar una serie de criterios lo más uniformes posibles, precisamente para evitar disparidades sobre si esas solicitudes de rectificación deben o no ser atendidas entre unos medios y otros.

En ese contexto, la Sala Tercera del Tribunal Supremo, cuenta ya con varios pronunciamientos en el ámbito de protección de estos derechos fundamentales, por ejemplo, en el ATS de 31 de mayo de 2019 (RCA 1074/2019, relativo a la protección de datos). Así, en lo que aquí interesa, cabe citar las sentencias relativas al derecho al olvido desde la perspectiva de la responsabilidad de los motores de búsqueda -por todas, STS n.º 1917/2016, de 21 de julio (RCA 2866/2015)- o desde la perspectiva de su ponderación con la veracidad de la información - STS nº. 12/2019, de 11 de enero (RCA 5579/2017)-; o la STS n.º 1407/2018, de 20 de septiembre (RCA 2828/2016) en la que la Sala repasa su jurisprudencia en este ámbito.

Es también ejemplo de lo anterior la reciente Sentencia la Sala de lo Contencioso del Tribunal Supremo, de 11.01.2019, por la que se desestima el recurso de casación interpuesto por Google frente a la sentencia de la Sección Primera de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 18 de julio de 2017, que confirma la obligación de desindexar ciertas informaciones que el Tribunal considera intromisivas en el honor del reclamante por imprecisas (se había acusado en una publicación a un guarda forestal de haber cazado de forma furtiva).

Ahondando en los principios sentados en la anterior Sentencia, de forma más reciente aún (5.7.2019), esa misma Sala ha dictado diversos Autos (Recursos de casación núm. 1733/2019 y 2099/2019) admitiendo a trámite otros recursos en los que estima existiría interés casacional, consistiendo dicho interés en: "precisar nuestra jurisprudencia sentada en la STS n.º 12/2019, de 11 de enero (RCA 5579/2017) a fin de:

> (i) Esclarecer si, ejercitado el derecho de cancelación ante el motor de búsqueda de Internet en relación con enlaces que contienen expresiones o manifestaciones hirientes sobre la persona del interesado, la ponderación entre los derechos fundamentales afectados debe realizarse:
>
> > a) entre el derecho a la protección de datos de carácter personal del interesado y el derecho a la información (en su doble vertiente: Google como motor de búsqueda y acceso a la información de los internautas), o bien
> >
> > b) entre el derecho a la protección de datos de carácter personal del interesado y el derecho a la libertad de expresión de Google como motor de búsqueda.

(ii) Precisar el contenido de los factores de ponderación relativos a la relevancia pública de la información, desde su perspectiva objetiva (actividad) y subjetiva (carácter público o privado de la persona afectada); así como la incidencia del factor tiempo en la calidad de los datos del interesado difundidos y en el ejercicio del derecho al olvido.

Precisa la Sala como "para ello será necesario interpretar el artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (a que remite el artículo 15 de la Ley Orgánica 3/2018, de 5 de diciembre), en relación con los artículos 18.4 y 20.1.a) y d) de la Constitución Española y la jurisprudencia que los interpreta".

Son esas resoluciones ejemplo de la construcción del cuerpo jurisprudencial, detallado y prolijo, al que venimos refiriéndonos, que aplica caso por caso los principios generales establecidos en materia de colisión de los derechos del art. 20 CE y art. 18 CE a la concreta materia de la autodeterminación informativa, y más exactamente, al denominado derecho "al olvido digital"[211].

4.5 Primer pronunciamiento del TEDH sobre el derecho al olvido digital: La Sentencia del TEDH de 28 de junio de 2018, M.L y W.W c/ Alemania

El 28 de junio de 2018 el TEDH se ha pronunciado por primera vez en un asunto en el que por los reclamantes se invocaba la vulneración del art. 8 del CEDH por motivo de la negativa de anonimización de determinadas informaciones incluidas en hemerotecas digitales, que les incumbían.

[211] SÁNCHEZ GÓMEZ, A., "Los derechos fundamentales a la intimidad, honor y protección de datos en la era digital: mecanismos jurídicos de protección, carencias y retos del legislador: de las leyes de 1982 (LOPHII) y de 1999 (LOPD) al Reglamento europeo de protección de datos de 2016", *Revista de Derecho Privado*, núm. 100, 2016, págs. 77-125.

4.5.1. Hechos y pronunciamientos del Tribunal Federal Alemán

Los hechos al origen del procedimiento seguido ante el TEDH son los siguientes.

En 1993, los reclamantes fueron condenados por el asesinato de un conocido actor y sentenciados al equivalente alemán de la cadena perpetua revisable. En 2007, cuando se acercaba la fecha se su salida de prisión, interpusieron distintos procedimientos frente a varios medios de comunicación [en particular, solicitando la anonimización de los archivos accesibles en sus hemerotecas online y fechados en el momento del juicio (un artículo, y un archivo de audio de un programa de radio y su transcripción[212])].

En 2009 y 2010, y a pesar de que en las instancias inferiores los reclamantes habían logrado obtener algunos pronunciamientos judiciales favorables a sus intereses, la Corte de Justicia Federal alemana revocó todas esas resoluciones de instancias inferiores dictando Sentencias en favor de los medios de comunicación, considerando:

- Que tanto el crimen como el juicio habían atraído considerable atención mediática en su momento, y que el público tenía interés en estar informado, lo que incluía la posibilidad de investigar el pasado.

- Que forma parte del rol de los medios de comunicación facilitar el acceso a sus archivos precisamente para participar en la formación de la opinión pública y el Estado democrático.

[212] En particular, los medios de comunicación en los que se publicaron esas informaciones fueron: Spiegel online, Deutschlandradio y Mannheimer Morgen.

- Que los reclamantes habían tratado, de forma relativamente reciente, de que su caso se reabriera, prácticamente tres años antes de ser puestos en libertad, solicitando de la prensa que informasen sobre esa solicitud de reapertura. Incluso la web de los abogados de uno de los condenados tenía hasta 2006, varios reportajes relativos a su cliente.

- En las publicaciones cuya anonimización se reclamaba se indicaba con claridad que se trataba de informaciones no recientes.

- También era preciso tener en cuenta que, en el caso de no contar con suficiente personal para atender las solicitudes de anonimización, los medios de comunicación podrían optar por no incluir en sus reportajes ningún elemento identificativo, y así evitar que con el paso del tiempo se vulnerase ningún derecho.

- El derecho de los reclamantes a la protección de su personalidad "debía ceder ante el derecho a la libertad de expresión de la estación de radio y ante el interés del público a estar informado".

Los reclamantes consideraron que la Corte Federal no había tenido en cuenta en su análisis la potencia de los motores de búsqueda en Internet y recurrieron el fallo de la Corte Federal ante el Tribunal Europeo de Derechos Humanos.

4.5.2. Fallo del TEDH

Ya hemos expresado que los reclamantes invocaban en su reclamación ante el TEDH la vulneración del art. 8 de la CEDH. Frente a tal pretensión, en el caso analizado, el TEDH determina que, en su criterio, Alemania no ha vulnerado tal derecho. Y ello considerando:

(i) El margen de apreciación de las autoridades nacionales respecto del balance a efectuar entre los derechos en juego.

(ii) La importancia de mantener disponibles publicaciones cuya legalidad no fue puesta en cuestión en el momento de su publicación.

(iii) La propia conducta de los reclamantes en relación con la prensa.

Por esas tres razones, la Corte no ve motivos sólidos por los que deba sustituir el criterio de los Tribunales alemanes por el suyo propio.

Además, puntualiza el TEDH **que las obligaciones de los motores de búsqueda respecto de las personas concernidas podrían ser distintas de las de los medios de comunicación al origen de esas informaciones,** pudiendo ser diferente el balance de los intereses en conflicto dependiendo de si los mismos involucran a quienes están "al origen y corazón de la libertad de expresión" o aquéllos cuyo objetivo no es publicar "sino facilitar su identificación y la localización de la información", pero subrayando asimismo que esos motores de búsqueda no habrían sido llamados al presente procedimiento ni se habría presentado ningún tipo de reclamación frente a los mismos.

En su fallo (el primero en el que el Tribunal Europeo de Derechos Humanos ha abordado expresamente la cuestión del derecho al olvido digital), el Tribunal Europeo de Derechos Humanos tiene en consideración los siguientes factores:

- Partiendo del convencimiento de que la publicación en los medios de comunicación de informaciones personales constituye una injerencia en la vida privada, **el TEDH examina el asunto desde la búsqueda del**

equilibrio entre el derecho al respeto de la vida privada del art. 8 del CEDH y la libertad de prensa y el derecho a la información del público[213].

- Sentado lo anterior, expone su asentada jurisprudencia sobre el papel relevante de los medios de comunicación en una sociedad democrática, como cuarto poder, y los criterios que ha considerado en el pasado cuando ha tenido que resolver un conflicto entre ambos derechos: el interés general del asunto: la notoriedad de la persona, el objeto del reportaje, el comportamiento previo de la persona afectada, el contenido, la forma y la repercusión de la publicación, así como, en último, término, las circunstancias en que obtuvo la información.

[213] En los casos que requieren un equilibrio entre el derecho al respeto de la vida privada y el derecho a la libertad de expresión, el Tribunal ha considerado siempre que el resultado de la solicitud de amparo no podría, en principio, variar según si el asunto le fue presentado, en virtud del artículo 8 del Convenio, por la persona que es el sujeto de la información o, en virtud del artículo 10, por el editor que lo publicó. Y ello porque, en principio, ambos derechos (arts. 8 y 10 de la CEDH) merecen igual respeto (Couderc y Hachette Filipacchi Associés v. Francia [GC], § 91, Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finlandia [GC], § 123; Medžlis Islamske Zajednice Brčko y otros Bosnia y Herzegovina [GC], § 77). Por lo tanto, el margen de apreciación debería ser, en principio, el mismo en ambos casos.
Los criterios relevantes definidos por la jurisprudencia para realizar el balance entre ambos derechos serían: a) la contribución a un debate de interés general; b) la notoriedad de la persona interesada; c) el objeto de la información; d) el comportamiento previo de la persona interesada; d) el contenido, la forma y la repercusión de la publicación. y, cuando corresponda, e) las circunstancias de la toma de las fotografías (ibid., §§ 90-93; Von Hannover v. Alemania (no. 2) [GC], §§ 108-113; Axel Springer AG v. Alemania [GC], §§ 89-95). Es reseñable la similitud que puede trazarse entre los criterios sostenidos por el TEDH en estas sentencias y los establecidos posteriormente para delimitar el alcance del derecho al olvido el TJUE en la *Sentencia Google*.
En el contexto de una solicitud del Artículo 10, el Tribunal también verifica como se obtiene la información y su veracidad y la gravedad de la pena impuesta a los periodistas o editores (Satakunnan Markkinapörssi Oy y Satamedia Oy v. Finlandia [GC], § 165).
Algunos de estos criterios pueden ser más o menos relevantes en las circunstancias particulares del caso (para un caso que involucra la recogida, procesamiento y publicación masiva de datos tributarios, ver ibid., § 166) y otros. los criterios también pueden aplicarse según el contexto (Medžlis Islamske Zajednice Brčko y otros v. Bosnia y Herzegovina [GC], § 88).
La Corte se pronunció sobre el alcance del derecho al respeto de la vida privada tal como está consagrado en el Artículo 8 en relación con el derecho a la libertad de expresión en virtud del Artículo 10, como servicios de la sociedad de la información como Google Inc. en el caso de Tamiz c. Reino Unido, así como respecto de un archivo en línea mantenido por los medios en el caso de M.L. y W.W. Alemania que estamos analizando.

Criterios que, considera el TEDH, pueden transponerse al asunto en cuestión, aunque algunos de los mismos puedan ser más o menos pertinentes en función de las circunstancias concurrentes.

- Y ello porque entiende el TEDH que "es preciso distinguir el papel de los medios de comunicación tradicionales y los medios digitales, habida cuenta de la mayor capacidad de difusión y permanencia de estos, lo que sin duda comporta un riesgo mayor para el derecho de respeto a la vida privada, sobre todo como consecuencia de los buscadores". "Pues una cosa es la injerencia inicial que resulta de la decisión de un medio de comunicación, incluso digital, de publicar una información y otra la que resulta de los buscadores, que no hacen sino amplificar el alcance de esa injerencia. Un efecto amplificador que, unido a la naturaleza diversa de la actividad que desarrollan, puede hacer que las obligaciones de los buscadores frente a la persona sobre la que se informa sean distintas de las del editor en origen de la noticia".

  De ahí que los resultados de una eventual demanda de cancelación puedan ser distintos según que se dirija contra el editor inicial de la información, cuya actividad se encuentra en el núcleo mismo de la libertad de expresión, o contra un buscador de Internet, cuyo interés principal no es publicar información inicial sobre la persona afectada, sino permitir, de una parte, recopilar toda la información disponible sobre una persona, y, de otra, establecer un perfil de la misma, haciéndose eco, a este respecto, de la jurisprudencia del Tribunal de Justicia de la Unión Europea.

- Partiendo de lo anterior, el Tribunal de Estrasburgo aplica al caso cada uno de los criterios citados más arriba:

- Respecto de la "contribución al debate general", la cuestión no se refiere al momento de su publicación, que nadie discute, sino el hecho de que sigan estando disponibles en Internet años después, en fechas próximas a la liberación de los demandantes. Es precisamente por ello por lo que concurre un interés legítimo de los demandantes en que se borren esos hechos de su pasado: facilitar su reintegración en la sociedad. Ahora bien, como hace notar el TEDH, también existe un legítimo interés de los ciudadanos en recibir información no solo sobre la actualidad sino también sobre acontecimientos del pasado.

  Ciertamente en este caso las partes no solicitan la supresión de los archivos litigiosos, sino que no figuren sus nombres, lo que por supuesto supondría una restricción menor para la libertad de prensa que la supresión sistemática del reportaje, pero recuerda que el modo en que se elabora una noticia y se define su contenido es parte indisoluble de la libertad de prensa, protegida por el art. 10 del CEDH.

  En concreto, la inclusión del nombre de la persona noticiable constituye un aspecto esencial del trabajo de la prensa y de la credibilidad de la noticia, máxime si se trata como en este caso de un procedimiento penal.

- Respecto de la "notoriedad" de los demandantes, el Tribunal de Estrasburgo concluye que, vista la notoriedad adquirida como consecuencia del crimen y del posterior proceso penal, no puede considerase que fueran personas desconocidas para el gran público en el momento de la presentación de la demanda ante el TEDH.

- En cuanto al "objeto de los reportajes", parece claro que tanto el proceso penal, como los recursos posteriores son elementos susceptibles de contribuir a un debate en una sociedad democrática. Respecto del comportamiento de los demandantes con respecto a la prensa, el TEDH destaca la circunstancia de que ellos mismos filtraron a la prensa numerosa documentación del proceso, así como el hecho de que figurara en la página web de uno de los abogados defensores numerosos reportajes sobre su cliente.

- En cuanto al "contenido, forma y repercusión de la publicación", ninguna duda hay sobre la veracidad y objetividad de los reportajes, mientras que el grado de difusión, que es lo que se cuestiona por los demandantes, es a juicio del TEDH limitado, vista su ubicación en la página web, pues no llamaría la atención de aquellos internautas que no buscaran específicamente información sobre los demandantes.

  Ciertamente, como señalan éstos, gracias a los buscadores de Internet se produce un efecto amplificador, dado que permite, independientemente del grado de difusión inicial, encontrar información sobre ellos de manera permanente, pero llegado a este punto, advierte el TEDH, no consta que los demandantes se hubieran dirigido previamente a las empresas que explotan los buscadores para reducir las posibilidades de que se encuentren esas informaciones sobre su persona, además de que el Tribunal no puede pronunciarse sobre la posibilidad de ordenar la adopción de otro tipo de medidas que supongan una

restricción menor a la libertad de expresión si no fueron objeto de debate previo en la jurisdicción nacional.

- **Un conjunto de consideraciones que llevan a Tribunal de Estrasburgo a concluir que**, visto el margen de apreciación de las autoridades nacionales, la importancia de mantener a disposición reportajes sobre cuya veracidad y objetividad nadie discute y el comportamiento de los demandantes con respecto a la prensa, **el estado alemán no habría faltado a su obligación de proteger su derecho a la vida privada**.

En el caso objeto de estudio, el TEDH analiza por primera vez un supuesto en el que se produce una colisión entre el derecho de información y el derecho al olvido digital, como variante del derecho fundamental a la intimidad/honor y derecho a la protección de los propios datos.

Como hemos visto, el asunto es muy específico, y por tal motivo ese Tribunal prima las libertades informativas, considerando el carácter noticiable que, con carácter general, se ha venido atribuyendo a los asuntos de naturaleza penal, así como el propio rol activo de los reclamantes de olvido en la "memoria" de esas informaciones (su papel activo en haberlas traído a la actualidad).

En todo caso, constituye un ejemplo más de la construcción jurisprudencial de este nuevo derecho, cuyo contenido y límites se están perfilando, caso por caso, a través de sentencias en ocasiones dispares y en las que, tienen la palabra no solo los Tribunales españoles en sus tres instancias (y varios órdenes jurisdiccionales), sino también nuestro Tribunal Constitucional y el Tribunal de Justicia de la Unión Europea y Tribunal Europeo de Derechos Humanos, entre todos los cuales se están sentando sus bases y estableciendo sus límites.

CAPÍTULO 5

LA REGULACIÓN DEL DERECHO AL OLVIDO EN LA NORMATIVA DE LA UNIÓN EUROPEA Y EN ESPAÑA.

SUMARIO: 5.1. LOS TRABAJOS PARA LA REVISIÓN DE LA DIRECTIVA 95/46/CE; 5.1.1. LA COMUNICACIÓN DE LA COMISIÓN EUROPEA DE 4 DE NOVIEMBRE DE 2010: UN ENFOQUE GLOBAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA UNIÓN EUROPEA; 5.1.2. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS SOBRE ESA COMUNICACIÓN; 5.1.3. RESOLUCIÓN DEL PARLAMENTO EUROPEO DE 6 DE JULIO DE 2011 SOBRE UN ENFOQUE GLOBAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA UNIÓN EUROPEA; 5.2. LA TRAMITACIÓN DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS; 5.3. EL ARTÍCULO 17 DEL RGPD; 5.3.1. RECONOCIMIENTO DEL DERECHO DURANTE LA TRAMITACIÓN DEL REGLAMENTO; 5.3.2. CONTENIDO DEL DERECHO AL OLVIDO; 5.4. RESTRICCIONES QUE CABE IMPONER AL DERECHO AL OLVIDO DIGITAL; 5.5. EL PROCEDIMIENTO PARA EJERCER EL DERECHO A LA SUPRESIÓN DE DATOS; 5.6. ORIENTACIONES DE LA COMISIÓN SOBRE LA APLICACIÓN DIRECTA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS A PARTIR DEL 25 DE MAYO DE 2018; 5.7 EL PAQUETE LEGISLATIVO DE REFORMA DE LA PROTECCIÓN DE DATOS APROBADO EN 2018; 5.8. EL REAL DECRETO-LEY 5/2018, DE 27 DE JULIO, DE MEDIDAS URGENTES PARA LA ADAPTACIÓN DEL DERECHO ESPAÑOL A LA NORMATIVA DE LA UNIÓN EUROPEA EN MATERIA DE PROTECCIÓN DE DATOS; 5.9. LA NUEVA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES: EL RECONOCIMIENTO POSITIVO DEL DERECHO AL OLVIDO DIGITAL EN LA LEGISLACIÓN ESPAÑOLA; 5.9.1. FASE DE TRAMITACIÓN DEL PROYECTO DE LEY ORGÁNICA; 5.9.2. CONTENIDO DE LA LEY ORGÁNICA; 5.9.3. RECONOCIMIENTO POSITIVO DEL DERECHO AL OLVIDO DIGITAL; 5.9.4. SENTENCIA 76/2019, DE 22 DE MAYO DE 2019., DEL PLENO DEL TRIBUNAL CONSTITUCIONAL

5.1 Los trabajos para la revisión de la Directiva 95/46/CE

La normativa comunitaria de protección de datos fue poco a poco quedando obsoleta, resultando precisa su adaptación para adaptarla a los nuevos desafíos a lo que tenía que hacer frente la materia como resultado del uso de las nuevas tecnologías y de la globalización.

No obstante, llama la atención la ausencia de referencias específicas al derecho al olvido digital en los trabajos previos a la revisión de la Directiva, que subraya el autor

ARTEMI RALLO[214], quien nos remite para constatar tal ausencia al Sumario de respuestas a la consulta pública sobre el futuro marco legal para la protección de datos[215], como a los dictámenes de las Autoridades Europeas de protección de datos a través del denominado Grupo de trabajo del art. 29.

Con esa consulta pública, la Comisión quería recabar la visión de los posibles interesados sobre los nuevos desafíos de la protección de datos a la luz de las nuevas tecnologías y de la globalización, tratando de recopilar información sobre la pregunta de si el marco legal vigente en ese momento podía afrontar esos retos y que tipo de acciones podrían ser requeridas en el futuro.

Ni en las respuestas formuladas por los interesados a esa Consulta pública de la Comisión, ni en el contenido de los Dictámenes del Grupo de trabajo del art 29 formulados con el mismo objeto se dejaba entrever, siquiera tangencialmente, mención alguna a ese derecho al olvido digital. Así resulta de la lectura del Dictamen de ese Grupo de trabajo[216] emitido con fecha de 1 de diciembre de 2009, titulado *"The future of privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data"*[217].

Una de las primeras referencias expresas al derecho al olvido digital fue formulada por la entonces vicepresidenta de la Comisión Europea, Viviane Reding, a principios de 2012, precisamente en el contexto de la revisión de ese marco normativo para adaptarlo a las implicaciones de las nuevas tecnologías y a la protección de datos en el entorno online.

---

[214] RALLO, A.: *El derecho al olvido en Internet. Google vs. España*. Colección "cuadernos y debates", Centro de Estudios Políticos y Constitucionales, Madrid, 2014.
[215] https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2009/consulting_0003_en
[216] Emitido de forma conjunta con el Grupo de trabajo de policía y justicia
[217] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp168_en.pdf

La entonces vicepresidenta de la Comisión señaló [218] que esa reforma debía incluir provisiones que garantizasen la retirada de datos personales en determinadas circunstancias:

> *"Another important way to give people control over their data: the right to be forgotten. I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to the processing of the personal data they have given out themselves"*[219].

Enfatizando seguidamente que ese derecho no es absoluto:

> *"There are cases where there is a legitimate and legally justified interest to keep data … The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right of the total erasure of history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media"*[220].

Sobre estas primeras aproximaciones al concepto de derecho al olvido digital, acertadamente señala ARTEMI RALLO en la obra ya citada que existía inicialmente una patente confusión entre los derechos al olvido y el derecho a la portabilidad de los datos, que asimismo reflejaba la preocupación latente en los ciudadanos de la Unión en ese momento, quienes en tanto que usuarios tenían que enfrentarse a grandes dificultades y obstáculos para poder cerrar cuentas en redes sociales, destruir sus datos, lograr el cambio de esos datos de una cuenta a otra, etc.

---

[218] Speech/12/26; Viviane Reding; Vice-President of the European Commission, EU Justice Commissioner; "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age"
http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

[219] *"Otra forma importante de dar a la gente control sobre sus datos personales: el derecho al olvido. Quiero clarificar expresamente que la gente debería tener el derecho -y no solo la posibilidad- de revocar el consentimiento al procesamiento de los datos personales que pudieran haber otorgado".*

[220] *"Hay casos en los que es legítimo y está justificado legalmente el derecho a conservar los datos… los archivos de un periódico son un buen ejemplo. Es claro que el derecho al olvido no puede derivar en un derecho al borrado total de la historia. Tampoco debe el derecho al olvido digital ser prevalente sobre los derechos a la libre expresión e información".*

Esa realidad, así como las denuncias formuladas al respecto por algunos particulares ante la Comisión Europea, se tradujo en la voluntad de las Instituciones comunitarias de atajar esas preocupaciones, facilitando a los usuarios el control efectivo de sus datos, sobre el nuevo concepto del derecho al olvido.

5.1.1 La Comunicación de la Comisión Europea de 4 de noviembre de 2010: Un enfoque global de la protección de los datos personales en la Unión Europea

En noviembre de 2010, la Comisión Europea publica su Comunicación *"un enfoque global de la protección de datos personales en la Unión Europea"*[221].

En esa Comunicación, y dentro de las medidas que deben implementarse para reforzar el control de los ciudadanos de la Unión Europea sobre sus propios datos -que es su objetivo fundamental-, se alude de forma expresa, por primera vez en un documento oficial de las Instituciones Europeas, al "derecho a ser olvidado".

Ese derecho se define en esa Comunicación como "el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos", aludiéndose, a título de ejemplo, al "caso en que la persona retira su consentimiento al tratamiento de datos, o del caso en que haya expirado el plazo de conservación de los datos". Respecto de ese derecho a ser olvidado, la Comisión subraya en esa Comunicación que "es preciso estudiar los medios que permitan esa clarificación".

[221] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Un enfoque global de la protección de los datos personales en la Unión Europea, de 4.11.2010
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0609&from=ES

Ese documento vincula el nacimiento del derecho al olvido al entorno online, desligándolo en cambio del concepto de portabilidad y aclarando la confusión existente en las primeras referencias a las que hemos aludido anteriormente.

5.1.2 Dictamen del Supervisor Europeo de Protección de datos sobre la Comunicación de la Comisión Europea de 4 de noviembre de 2010

Sobre esa Comunicación, emitió un Dictamen el Supervisor Europeo de protección de datos con fecha de 22 de junio de 2011[222]. En ese Dictamen señalaba que la regulación del derecho al olvido permitiría garantizar que la información almacenada relativa a un usuario "desapareciese automáticamente al cabo de un determinado período, incluso si el interesado no realiza ninguna acción en este sentido o desconoce que los datos fueron almacenados", incidiendo en los beneficios que podría tener la codificación de ese nuevo "derecho al olvido".

En particular, el Supervisor Europeo de Protección de Datos subraya como la codificación de ese derecho, que califica de "útil" y "merecedor de ser incluido en un instrumento jurídico", garantizaría la supresión de los datos (y la prohibición de su uso posterior) sin necesidad de acción alguna por parte del interesado, atribuyéndoles lo que en ese Dictamen se denomina como "una especie de fecha de caducidad". Se trataría de una "situación asimilable a la de la cancelación de antecedente penales o disciplinarios" que permitiría su cancelación de un modo "objetivo" y "automatizado".

[222] Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — *«Un enfoque global de la protección de los datos personales en la Unión Europea»* (2011/C 181/01) https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_es.pdf

En virtud de ese nuevo derecho, el responsable del tratamiento podría conservarlos solo en circunstancias muy concretas, "en las que pueda determinarse una necesidad específica de conservarlos durante un período de tiempo más prolongado". En consecuencia, el "derecho al olvido" invertiría la carga de la prueba de la persona hacia el responsable del tratamiento y constituiría un «derecho a la intimidad por defecto» establecido para el tratamiento de datos personales.

En el criterio del Supervisor, ese derecho sería especialmente útil en el contexto de los servicios de la sociedad de la información, en los medios de comunicación, Internet y las redes sociales. Sería también interesante para garantizar que los datos almacenados en dispositivos móviles y ordenadores se borran pasado un periodo de tiempo determinado. Así, ese derecho podría interpretarse como una obligación de "intimidad mediante el diseño".

5.1.3 Resolución del Parlamento Europeo de 6 de julio de 2011 sobre un enfoque global de la protección de los datos personales en la Unión Europea:

Esa Comunicación recibió asimismo el refrendo del Parlamento Europeo a través de la Resolución de 6 de julio de 2011, *sobre un enfoque global de la protección de los datos personales en la Unión Europea* (2011/2025(INI))[223], que "acoge con gran satisfacción" y "apoya" el enfoque de esa publicación, manifestando su "pleno compromiso" con el enfoque dado al texto por la Comisión Europea, al entender que "las normas y los principios que establece la Directiva 95/46/CE representan un punto de partida ideal y deberán detallarse, ampliarse y observarse como parte de una legislación moderna en materia de protección de datos", incidiendo en la necesidad de reforzar los derechos de

[223] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES

las personas (garantía de los derechos, sencillez y gratuidad en su ejercicio), así como en la necesidad de "seguir avanzando en la dimensión del mercado interior" y "garantizar una mejor aplicación de las normas de protección de datos" en todos los Estados miembros.

5.2. La tramitación del Reglamento Europeo de Protección de datos

El 25 de enero de 2012 la Comisión Europea presentó un proyecto de *Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*[224].

Ese primer borrador ya incluía, dentro de su Sección 3ª ("rectificación y supresión") y con base en el art.12, letra b), de la Directiva 95/46/CE, un artículo 17, que establecía el derecho del interesado "al olvido" y "supresión". Derecho entendido como "la obligación del responsable del tratamiento que haya difundido los datos personales de informar a los terceros sobre la solicitud del interesado de suprimir todos los enlaces a los datos personales, copias o réplicas de los mismos", integrando "el derecho a que se restrinja el tratamiento en determinados casos", "evitando la ambigüedad del término «bloqueo»"[225].

La norma se tramitó a través del procedimiento legislativo ordinario (procedimiento de codecisión)[226], transmitiéndose al Parlamento Europeo y al Consejo el 27 de enero de 2012.

[224] Reglamento General de protección de datos/* COM/2012/011 final - 2012/0011 (COD) */ https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0011&from=en
[225] Considerandos 53, 54 y 129.
[226] El proyecto de tramitación del Reglamento está contenido en el siguiente enlace: https://eur-lex.europa.eu/procedure/EN/2012_11

Entre los meses de marzo y octubre de 2012 se recabó la opinión del Supervisor Europeo de protección de datos, del Comité Europeo Económico y Social, y del Comité de las Regiones. Adoptándose en primera lectura en el PE en marzo de 2014. Sobre las enmiendas introducidas al texto de la Comisión por el PE en esa primera lectura se pronunció la Comisión con fecha de junio de 2014 -alcanzándose un acuerdo parcial-, y en segunda lectura en abril de 2016, publicándose en el DOCE el 4 de mayo de 2016.

La versión final del texto del Reglamento, tras varias modificaciones sufridas durante el procedimiento de tramitación legislativa que veremos en el epígrafe siguiente de este Capítulo, incorporó en su artículo 17 el reconocimiento del derecho al olvido en los siguientes términos:

> ***"Artículo 17.- Derecho de supresión («el derecho al olvido»)***
>
> *1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:*
>
> > *a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;*
> >
> > *b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;*
> >
> > *c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;*

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

> *d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o*
>
> *e) para la formulación, el ejercicio o la defensa de reclamaciones".*

A ese derecho, avatares de su tramitación legislativa, objetivos y contenido dedicaremos el apartado siguiente del presente Capítulo.

Sobre la aplicación de ese Reglamento[227] la Comisión publicó una comunicación al Parlamento y al Consejo, con Orientaciones sobre su aplicación directa, el 24 de enero de 2018.

El mismo, se aplica de forma directa en todos los Estados miembros de la UE desde el 25 de mayo de 2018. Sin perjuicio de esa aplicación directa, algunos Estados miembros han aprobado -o están aprobando- normas para la adaptación de su normativa interna al contenido del RGPD de la Unión Europea. Son ejemplos:

- La Ley *Act to Adapt Data protection Law to regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680*[228] aprobada por Alemania en junio de 2017 y con la que, como se indica en su propio título, se han adaptado las disposiciones de la Ley Federal de Protección de Datos al Reglamento UE objeto de este Proyecto de Ley.

[227] https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0043&qid=1517578296944&from=EN
[228] http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/44.pdf

- En Francia, la adaptación de las disposiciones del Reglamento 2016/679/UE se ha llevado a cabo mediante la modificación de algunos preceptos de la *Loi 78-17 du 6 janvier relative à l'informatique, aux fichiers et aux libertés* (en especial los artículos 1, 32, 40-1 o 43); y de algunas disposiciones introducidas en la *Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique*. El impacto del Reglamento sobre la legislación francesa aparece detallado en el Anexo 1 del Informe de la Asamblea Nacional que puede consultarse pinchando sobre el enlace que incluimos al pie de esta página[229].

- En Italia se ha aprobado una Guía elaborada por la autoridad Garante per la protezione dei dati personali, *Guida all applicazione del Regolamento UE 2016/679*[230], en la que la Autoridad explica las modificaciones que traerá consigo la aplicación del Reglamento a particulares y empresas, al tiempo que ofrece recomendaciones para cada uno de los aspectos de la reforma.

- Gran Bretaña tramita actualmente en el Parlamento la *Data Protection Bill*[231], que modifica su legislación de protección de datos, incorporando los preceptos del Reglamento UE.

- En Portugal, acaba de aprobarse (junio 2019) la Ley 58/2019[232], *por la que se garantiza la aplicación, en el ordenamiento jurídico nacional, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Esta norma ha sustituido la hasta hace poco vigente

[229] http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/48.pdf
[230] https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf
[231] http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/49.pdf
[232] https://dre.pt/web/guest/home/-/dre/123815982/details/maximized

Ley de Protección de Datos (LPD) - Ley 67/98, de 26 de octubre[233], que seguía en vigor en todo aquello en lo que no era contraria al RGPD.

La nueva norma asegura la ejecución legislativa referida en el RGPD, aunque su tramitación ha seguido un camino difícil, ya que ha encontrado reparos por parte de la propia CNPD, que ha señalado la existencia de violaciones constitucionales, normas contradictorias e incluso ha propuesto modificaciones y supresiones de artículos[234].

[233] Lei n.° 67/98 de 26 de Outubro (Dados pessoais)
http://www.wipo.int/wipolex/es/text.jsp?file_id=206648

[234] De forma paralela a la tramitación de esa norma, y en el mes de octubre de 2018, se ha producido la primera sanción por parte de la CNPD en aplicación de ese RGPD.
La Comisión Nacional de Protección de Datos impuso multas por importe de 400.000 € al Centro Hospitalario Barreiro-Montijo, debido a las políticas de acceso a las bases de datos de ese hospital, que permitían a técnicos y médicos consultar los procesos clínicos de los pacientes sin la debida autorización. La multa es el resultado de una inspección llevada a cabo a consecuencia de una denuncia de la Orden de Médicos el pasado mes de junio, y se impuso por la CNPD a la luz del RGPD. La resolución, de fecha 11.10.2018, señala que al menos nueve profesionales con funciones en el área de los servicios sociales disponían de accesos que deberían ser exclusivos de los médicos. La CNPD también justificó la imposición de las sanciones en el hecho de que se registraron 985 médicos con cuentas activas que daban acceso a los archivos clínicos, aunque los cuadros del Hospital del Barreiro solo cuentan con 296 médicos contratados (la disparidad entre el número de cuentas y el número de médicos se relacionará con los pasos temporales determinados por el sistema de colocación de los profesionales de la salud).
La decisión revela además que, en una cuenta de prueba, los expertos de la CNPD lograron acceder a datos clínicos de un paciente, que se encontraban en los archivos digitales del Hospital de Santa Cruz, en Carnaxide. Además, el hospital no disponía de reglas internas para la creación de cuentas (que se crearon después del envío de e-mails por los diferentes directores de los servicios) o para los diferentes niveles de acceso a la información clínica, y el método de autenticación no tenía en cuenta los datos identificativos que vinculan a los diferentes profesionales al hospital.
La CNPD consideró probada la existencia de tres infracciones: de los principios de integridad y confidencialidad; del principio de minimización de datos que debería impedir el acceso indiscriminado a datos clínicos de los pacientes; incapacidad del responsable del tratamiento de datos para garantizar la confidencialidad y la integridad de los datos. Las dos primeras infracciones fueron sancionadas con multas de 150.000 euros cada una, mientras que la tercera representó un incremento de 100.000 euros.

5.3 Contenido del art. 17 del RGPD

5.3.1 Reconocimiento del derecho al olvido durante la tramitación del Reglamento[235]

La redacción del art. 17 del RGPD contenida en la primera propuesta de texto reglamentario formulado por la Comisión Europea el 25 de enero de 2012, era sustancialmente más larga que el texto de la versión definitiva.

Particularmente, contaba con nueve numerales en los que, bajo la rúbrica "derecho al olvido y a la supresión", se recogían los supuestos en los que el responsable del tratamiento debía suprimir los datos del interesado (apartado 1º), que en la propuesta original eran cuatro en vez de seis. También se incluían tres apartados en los que se hacía referencia a limitaciones del tratamiento por parte del responsable y características, en los apartados 4, 5 y 6. Además de lo anterior, el texto propuesto por la Comisión recogía en sus apartados 7, 8 y 9 la garantía del respeto a los plazos de supresión, la imposibilidad de emplear los datos suprimidos para cualquier otro destino, regulándose en el noveno y último apartado la potestad de la Comisión para adoptar actos delegados a fin de especificar criterios relativos a "sectores y situaciones específicos de tratamiento de datos", "las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público" y "criterios y condiciones para limitar el tratamiento de datos personales" en relación con las excepciones contenidas en el apartado 4º original.

La tramitación continuó con la aprobación del texto con enmiendas en primera lectura, el 12 de marzo de 2014, en el Parlamento Europeo[236]. De las

[235] https://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/

[236] Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014*, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al*

enmiendas aprobadas por el Parlamento Europeo destaca la supresión del término "olvido" del encabezamiento del artículo, añadiendo una obligación a terceros de que eliminen todos los enlaces, copias y réplicas cuando concurran las circunstancias que se explicitan. En particular, se incluyó el supuesto de que una autoridad administrativa haya resuelto de manera firme que esos enlaces deban ser anulados. Asimismo, el Parlamento propuso eliminar el apartado 7 de la propuesta de la Comisión y añadir un apartado 8.bis, según el cual el responsable del tratamiento tendría que implementar las medidas correctivas en un determinado plazo y verificar periódicamente la adecuación de los datos.

El 15 de junio de 2015 el Consejo de la UE adoptó un primer acuerdo sobre el texto y da al Presidente del Consejo el mandato de entrar en negociaciones con el Parlamento Europeo.

El 18 de diciembre de 2015, Consejo y Parlamento alcanzaron un acuerdo sobre el texto del RGPD.

El 8 de abril de 2016, el Consejo de la UE adoptó su posición respecto de ese reglamento en primera lectura[237], siendo su redacción la más parecida a la que fue aprobada finalmente y entró en vigor en mayo de 2018.

El 27 de abril de 2016 se firmó el texto definitivo por el Presidente del Parlamento Europeo y el del Consejo, publicándose en el Boletín Oficial de

tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura)
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014AP0212&from=EN

[237] Posición del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE* (Reglamento General de protección de datos).
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_5419_2016_REV_1&from=EN

las Comunidades Europeas el 4 de mayo de 2016. El RGPD entra en vigor el 24 de mayo de 2016 (veinte días después de su publicación en el DOCE) y se aplica directamente en todo el territorio de la UE a partir del 25 de mayo de 2018 (dos años después a contar desde el día siguiente al de su entrada en vigor).

Poco después de la entrada en vigor del Reglamento a mediados de 2016, la Comisión inició el trabajo con las autoridades de los Estados miembros, las autoridades de protección de datos y las partes interesadas para preparar la aplicación del Reglamento y proporcionar apoyo y asesoramiento.

En ese contexto, la Comisión ha colaborado estrechamente con los Estados miembros para apoyar su trabajo durante el período transitorio, con el fin de garantizar el nivel más elevado posible de coherencia. A tal fin, la Comisión ha creado un grupo de expertos encargado de acompañar a los Estados miembros en su labor de preparación para el Reglamento. El grupo, que se ha reunido hasta en trece ocasiones hasta el mes de enero de 2018, actúa como foro en el que los Estados miembros pueden compartir sus experiencias y conocimientos. La Comisión ha participado también en reuniones bilaterales con las autoridades de los Estados miembros para debatir cuestiones que surgen a nivel nacional, apoyando además activamente la labor del Grupo de trabajo del artículo 29[238], también con vistas a facilitar la transición al Comité Europeo de Protección de Datos.

[238] Orientaciones/documentos de trabajo del Grupo de trabajo del artículo 29 elaborados con vistas a la aplicación del RGPD: 1) Derecho a la portabilidad de los datos; 2) Delegados de protección de datos; 3) Nombramiento de la autoridad de control principal; 4) Evaluación de impacto relativa a la protección de datos; 5) Multas administrativas; 6) Elaboración de perfiles; 7) Violación de la seguridad de los datos; 8) Consentimiento; 9) Transparencia; 10) Certificación y acreditación; 11) Referencias sobre adecuación; 12) Normas corporativas vinculantes para los responsables del tratamiento; 13) Normas corporativas vinculantes para los encargados

Hemos elaborado un cuadro comparativo de la evolución de la redacción del art. 17 del RGPD según las propuestas de la Comisión Europea, Parlamento y Consejo, que es ilustrativo de la evolución del contenido de ese artículo durante su tramitación legislativa, que hemos relatado en el presente apartado, y que se anexa al presente trabajo de tesis como Anexo 1.

5.3.2 Contenido del derecho al olvido

El artículo 17 del Reglamento se subdivide en tres apartados:

En el primero, se establece el derecho del interesado a la supresión de datos por parte del responsable del tratamiento cuando concurran una serie de circunstancias: 1) que los datos ya no sean necesarios para los fines para los que fueron recogidos; 2) la revocación del consentimiento del interesado; 3) oposición del interesado; 4) tratamiento ilícito de datos; 5) cuando los datos deban suprimirse para cumplir una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; 6) cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1 del Reglamento.

En el segundo apartado, se dispone la obligación del responsable del tratamiento de "adoptar medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos".

En el tercer y último apartado de ese artículo 17 se disponen excepciones a las disposiciones de los dos apartados anteriores, y en particular, que los mismos

no se aplicarán: 1) cuando el tratamiento sea preciso para ejercer el derecho a la libertad de expresión e información; 2) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; 3) por razones de interés público en el ámbito de la salud pública; 4) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho al olvido "pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento"; finalmente 5) para la formulación, el ejercicio o la defensa de reclamaciones.

Según de deriva de la redacción del art. 17 del RGPD, el derecho al olvido es un derecho sujeto a limitaciones, estando el responsable obligado a eliminar los datos solo cuando concurran algunas de las condiciones contenidas en el apartado 1º del art. 17, pero no debiendo hacerlo cuando nos hallemos ante las excepciones contenidas en el apartado 3º de ese mismo artículo.

La formulación de este nuevo derecho no está exenta de excepciones susceptibles de interpretación jurisprudencial, y que variará en función de las circunstancias de uno u otro supuesto, determinando la necesidad de la intervención de los jueces nacionales en la fijación de sus perfiles exactos.

Asimismo, cabe destacar, como hace ÁLVAREZ CARO[239], que es el responsable del tratamiento quien debe efectuar esa supresión, entendiendo esa figura del responsable como una figura amplia y que incluiría a "todo prestador de servicios de la sociedad de la información", como son: redes sociales, blogs, plataformas de comercio electrónico, etc.

[239] PIÑAR MAÑAS, J.L. (Director) y ÁLVAREZ CARO, M./RECIO GAYO, M. (Coordinadores): *Reglamento General de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Ed. Reus, Madrid 2016. Pág. 247

> El derecho al olvido se consagra como un nuevo derecho en el RGPD, pero no deja de ser, como ha indicado la doctrina mayoritaria[240], un derecho nuevo manifestación de otros derechos y principios ya existentes, como el derecho de cancelación, el principio de calidad de los datos, tratándose "de la propia evolución de los derechos de cancelación y oposición, al compás del avance de las nuevas tecnologías y del avance de Internet"[241].

5.4 Restricciones que cabe imponer al derecho al olvido digital

Interesa destacar, asimismo, que el RGPD establece, en su art. 23, que es posible establecer limitaciones a los derechos y obligaciones reconocidos en los artículos 12 a 22 de esa norma.

Particularmente, resulta posible establecer esas restricciones cuando las mismas sean precisas para: proteger la seguridad del Estado; con fines de defensa; seguridad pública; prevención; investigación; detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales; otros objetivos de interés público general de la Unión o de un Estado miembro -en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; la protección de la independencia judicial y de los procedimientos judiciales; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública; la protección del interesado o de los derechos y libertades de otros; y la ejecución de demandas civiles.

---

[240] PIÑAR MAÑAS, ARTEMI RALLO o NIEVES BUISÁN son ejemplos.
[241] ÁLVAREZ CARO, infra 146.

Sobre esos aspectos, enumerados en las letras a) a j) del apartado 1º del art. 23 del RGPD, dispone el numeral segundo de ese mismo artículo que "cualquier medida legislativa indicada en el apartado 1" "contendrá como mínimo" "disposiciones específicas relativas a": a) la finalidad del tratamiento o de las categorías de tratamiento; b) las categorías de datos personales de que se trate; c) el alcance de las limitaciones establecidas; d) las garantías para evitar accesos o transferencias ilícitos o abusivos; e) la determinación del responsable o de categorías de responsables; f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento; g) los riesgos para los derechos y libertades de los interesados, y h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta".

5.5 El procedimiento para ejercitar el derecho a la supresión de datos de carácter personal

Respecto del procedimiento para ejercitar el derecho a la supresión de datos, establecido en el art. 12 del RGPD, interesa al objeto de este trabajo destacar que el interesado podrá ejercitarlo, en primer lugar, ante el responsable de ese tratamiento, quien debe facilitar al interesado la información relativa a sus actuaciones respecto de esa solicitud en el plazo máximo de un mes desde la recepción de esa solicitud. Dicho plazo podrá prorrogarse otros dos meses "en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes". El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se le faciliten de otro modo.

Según se establece en el apartado 4º de ese artículo 12, "si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales".

El responsable del tratamiento deberá realizar todas esas actuaciones a título gratuito, y cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. Sin embargo, el responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

En la hipótesis de que el responsable del tratamiento tenga dudas razonables sobre la identidad de la persona física que cursa la solicitud, podría solicitarle información adicional para confirmar su identidad.

También establece el RGPD que la información normalizada que debe transmitirse podrá hacerse en combinación con iconos normalizados que permitan proporcionar "de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto". Los iconos que se presenten en formato electrónico deberán ser legibles mecánicamente, pudiendo la Comisión "adoptar actos delegados" para especificar "la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados".

5.6. Orientaciones de la Comisión sobre la aplicación directa del Reglamento General de protección de datos a partir del 25 de mayo de 2018

El Reglamento General de protección de datos, en tanto que actos legislativo vinculante, se aplica en su integridad en toda la UE sin necesidad de trasposición. Esa pieza de legislación constituye la más importante novedad normativa en el ámbito de la protección de datos de los últimos veinte años.

Como continuación a la misma, en el mes de enero de 2018 la Comisión Europea publicó una Comunicación en la que se contienen sus orientaciones sobre la aplicación directa del Reglamento General de protección de datos a partir del 25 de mayo de 2018[242].

En esa Comunicación, la Comisión Europea "recapitula las principales innovaciones y oportunidades que ofrece la nueva legislación de la UE en materia de protección de datos"; "evalúa los trabajos preparatorios realizados hasta la fecha a nivel de la UE"; "resume todo aquello que la Comisión Europea, las autoridades nacionales de protección de datos y las administraciones nacionales tienen aún pendiente para llevar a buen término la preparación"; y "establece las medidas que la Comisión tiene previsto adoptar en los próximos meses". Exponiendo asimismo como "de manera paralela a la adopción de esa Comunicación", "la Comisión pone en marcha una serie de herramientas en línea para ayudar a las partes interesadas a prepararse para la aplicación del Reglamento y, con la ayuda de las oficinas de representación, una campaña de información en todos los Estados miembros".

[242] Comunicación de la Comisión al Parlamento Europeo y al Consejo: "Mayor protección, nuevas oportunidades: Orientaciones de la Comisión sobre la aplicación directa del Reglamento General de protección de datos a partir del 25 de mayo de 2018"
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN

El contenido más relevante de esa Comunicación es el relativo a las medidas pendientes para la correcta implantación del Reglamento, destacando las que siguen:

i. Ultimar el establecimiento de un marco jurídico nacional por parte de los Estados miembros.

Sobre este objetivo la Comunicación destaca que a pesar de ser el Reglamento directamente aplicable en todos los Estados miembros, éstos han de adoptar las medidas necesarias para adaptar su legislación mediante la derogación y modificación de las leyes existentes, así como implantando autoridades nacionales de protección de datos en aquéllos países en los que éstas no existan, eligiendo un organismo de acreditación y estableciendo las normas para la conciliación de la libertad de expresión y la protección de los datos.

La Comunicación también destaca la oportunidad que el Reglamento supone para que los Estados miembros precisen aún más la aplicación de las normas de protección de datos en sectores específicos tales como: el sector público, el empleo y la seguridad social, medicina preventiva y medicina laboral, sanidad pública, archivo con fines de interés público, investigación científica o histórica o con fines estadísticos, número nacional de identificación, acceso público a los documentos oficiales u obligaciones de secreto. Además, en el caso de los datos genéticos, datos biométricos y datos relativos a la salud, el Reglamento autoriza a los Estados miembros a mantener o introducir condiciones adicionales, inclusive limitaciones.

En resumen, "el Reglamento supone la oportunidad para simplificar el entorno jurídico y, en consecuencia, tener un menor número de normas nacionales y una mayor claridad para los operadores".

Igualmente se indica por la Comisión que, al corresponder la interpretación del Reglamento a los órganos jurisdiccionales europeos (los tribunales nacionales y, en última instancia, el Tribunal de Justicia de la Unión Europea) y no a los legisladores de los Estados miembros, estos últimos no pueden "ni copiar el texto del Reglamento cuando no sea necesario a la luz de los criterios establecidos por la jurisprudencia", "ni interpretarlo o añadir condiciones adicionales a las normas directamente aplicables en virtud del Reglamento", ya que si lo hicieran, los operadores de toda la Unión se enfrentarían de nuevo a una situación de fragmentación y no sabrían qué normas deben cumplir.

La Comisión recoge en su Comunicación que solo dos Estados miembros habían adoptado a la fecha de publicación de esa Comunicación la legislación nacional pertinente (Austria y Alemania); y que el resto de Estados miembros se encontraban en distintas etapas de sus procedimientos legislativos, teniendo programado adoptar la legislación antes del 25 de mayo de 2018.

Finalmente destaca la Comisión en esa Comunicación que "en caso de que los Estados miembros no adopten las medidas necesarias requeridas en virtud del Reglamento, se retrasen en su adopción o hagan uso de las cláusulas de especificación previstas en el Reglamento de manera contraria a lo dispuesto en él, la Comisión hará uso de todos los instrumentos que tiene a su disposición, incluido el recurso al procedimiento de infracción".

ii. La garantía por parte de las autoridades de protección de que el nuevo Comité Europeo de Protección de Datos independiente sea plenamente operativo.

Respecto de esta necesidad destaca la Comisión que el Comité Europeo de Protección de Datos "será el punto de referencia de la protección de datos en Europa", contribuyendo "a una aplicación coherente de la legislación en

materia de protección de datos" y proporcionado "una base sólida para la cooperación entre las autoridades de protección de datos, incluido el Supervisor Europeo de Protección de Datos". El Comité Europeo de Protección de Datos publicará orientaciones sobre la forma de interpretar los conceptos básicos del Reglamento y decisiones vinculantes sobre conflictos relativos al tratamiento transfronterizo, con el fin de garantizar la aplicación uniforme de las normas de la UE y evitar que el mismo caso se trate de forma diferente en los distintos Estados miembros.

El Comité Europeo de Protección de Datos deberá "crear una cultura común de protección de datos entre todas las autoridades nacionales de protección de datos para garantizar que las disposiciones del Reglamento se interpretan de manera coherente", por lo que la Comisión "anima a las autoridades de protección de datos a adoptar estos cambios y a adaptar su funcionamiento, su financiación y su cultura de trabajo para poder cumplir con los nuevos derechos y obligaciones".

iii. Necesidad de que los Estados miembros faciliten recursos económicos y humanos a las autoridades nacionales de protección de datos

La Comunicación señala a las autoridades nacionales de protección de datos como "los interlocutores naturales y el primer punto de contacto para los ciudadanos, las empresas y las administraciones públicas en cuanto a consultas relacionadas con el Reglamento". También señala la importancia de su papel respecto de acciones de sensibilización e información, comprensión de normas, y en general, actividades tendentes a la salvaguarde los derechos y libertades individuales, lo cual no es posible, "a menos que actúen con total independencia".

Por ello, y para poder hacer frente a las competencias que les atribuye el Reglamento (tratar de manera efectiva las reclamaciones, llevar a cabo investigaciones eficaces, tomar decisiones vinculantes e imponer sanciones efectivas y disuasorias), se anima a los Estados miembros "a cumplir con su obligación legal de proporcionar a su autoridad nacional de protección de datos los recursos humanos, técnicos y financieros, así como las instalaciones e infraestructuras, necesarios para el desempeño efectivo de sus funciones y el ejercicio de sus competencias".

iv. Preparación por parte de empresas, organizaciones y administraciones públicas a la administración de las nuevas normas. Información a ciudadanos y PYMES.

La Comisión incide en la necesidad de que los operadores se preparen y se adapten a las nuevas reglas contenidas en el Reglamento, concibiendo esa adaptación como: a) una oportunidad para poner orden en sus actividades en lo referente a los datos personales que tratan y la forma en la que lo gestionan; b) una obligación para desarrollar productos compatibles con la privacidad y la protección de los datos y para construir una nueva relación con sus consumidores basada en la transparencia y la confianza; y c)·una oportunidad para restablecer sus relaciones con las autoridades de protección de datos a través de la rendición de cuentas y el cumplimiento proactivo.

Además, deben intensificarse las campañas de formación puestas en marcha por las autoridades de protección de datos, con especial hincapié en ciudadanos y PYMES, considerando que el éxito del Reglamento depende de la adecuada sensibilización de todos aquellos a quienes conciernen las nuevas normas (particularmente, la comunidad empresarial y otras organizaciones que realizan el tratamiento de datos, el sector público y los ciudadanos).

Desde la fecha de aplicación del RGPD (25 de mayo de 2018), la Comisión supervisará la efectiva aplicación de sus normas, con el fin de tomar medidas en el caso de que surgieran problemas que justificasen esa intervención.

Un año después de esa fecha de aplicación (mayo de 2019), la Comisión tenía previsto organizar un acto para hacer balance de las experiencias de las distintas partes interesadas por lo que respecta a la aplicación del Reglamento. Lo que tuvo lugar finalmente el día 13 de junio de 2019 pasado[243].

Ese balance se incorporará también al informe que la Comisión debe preparar para mayo de 2020 sobre la evaluación y revisión del Reglamento, que se centrará, en concreto, en las transferencias internacionales y en las disposiciones sobre cooperación y coherencia que atañen al trabajo de las autoridades de protección de datos[244].

5.7. El paquete legislativo de reforma de la protección de datos aprobado en 2018

Resulta también interesante mencionar que con posterioridad a la aprobación del RGPD, y al margen de los trabajos de implementación de esa norma en los Estados miembros, siguen llevándose a cabo otros avances en materia de protección de datos por las Instituciones Europeas.

En particular, interesa a los efectos del presente trabajo destacar que el 6 de abril de ese mismo año 2016, se había adoptado por parte de la UE el paquete legislativo de reforma de la protección de datos, que incluía, además del Reglamento General de

[243] "One year of GDPR application: taking stock in the EU and beyond". https://ec.europa.eu/info/events/gdpr-stock-taking-event-2019-jun-13_en
[244] BENITO MARTÍN, R.: *La evaluación del impacto en protección de datos tras el RGPD*. Certamen de artículos jurídicos sobre Derecho del entretenimiento 2016 Premios DENAE, Ed. DENAE, Madrid 2016.

protección de datos (RGPD) -que venimos de analizar -, la Directiva sobre la cooperación policial[245].

Además de esa Directiva, en el ámbito de la protección de datos (en constante actualización y reforma), se está tramitando también actualmente una revisión del texto del Reglamento revisado para las instituciones, órganos y organismos de la UE[246] y un Reglamento sobre la privacidad y las comunicaciones electrónicas[247], que se encuentran actualmente en fase de negociación[248].

Estas propuestas normativas completarían las previsiones del RGPD, "ampliando su ámbito de aplicación a todos los proveedores de servicios de comunicaciones electrónicas, así como a los proveedores de programas informáticos que permiten acceder a servicios de comunicaciones electrónicas, incluyendo la recuperación y presentación de información de Internet"[249], en palabras de PANIZA FULLANA.

Una vez adoptados esos textos legales, garantizarán que la UE esté dotada de un conjunto de normas de protección de datos sólido y completo.

---

[245] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

[246] Propuesta de Reglamento del Parlamento Europeo y del Consejo *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión 1247/2002/CE*, COM(2017) 8 final.

[247] El estado de tramitación de la norma puede consultarse en: https://eur-lex.europa.eu/legal-content/ES/HIS/?uri=CELEX:52017PC0010

[248] La propuesta de texto revisado de esa Directiva se publicó el 22 de julio de 2016, y fue adoptado por la Comisión el 11 de enero de 2017.

[249] BARRIO ANDRÉS, M. en *Internet de las cosas* (pág. 79, Ed. Reus, Madrid 2018), con cita a PANIZA FULLANA, A.: "Una nueva era en la privacidad y las comunicaciones electrónicas: La Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto a la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas", en *Revista Doctrinal Aranzadi Civil-Mercantil*, nº 7/2017, 2017.

5.8. El Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos[250]

La entrada en vigor en España el 25 de mayo de 2018 pasado del RGPD de la UE, supuso el desplazamiento de todas las disposiciones de Derecho interno que no se acomodasen a lo dispuesto en el aludido reglamento comunitario. Esta circunstancia tuvo, sin duda, impacto sobre muchos preceptos tanto de la LOPD como de su reglamento de desarrollo (RD 1720/2007).

Por otra parte, numerosos preceptos del reglamento europeo se remiten a su desarrollo, obligatorio o potestativo, por los Estados miembros, conteniendo hasta cincuenta y seis remisiones a los ordenamientos nacionales. Entre esas remisiones se encuentra la imposición a los Estados miembros de regular el estatuto de las autoridades de control, la determinación del régimen aplicable a los inspectores de un tercer Estado que lleven a cabo actividades conjuntas de investigación o la designación de la autoridad que representará al Estado miembro en el Comité Europeo de Protección de Datos.

Además de lo anterior, hay otras disposiciones del Reglamento General de protección de datos que exigen una adecuación del Derecho interno, como lo es el régimen sancionador, que tipifica las conductas que pueden ser objeto de sanción, pero no regula cuestiones tales como sus plazos de prescripción, que asume corresponden a los ordenamientos internos de los Estados Miembros. También establece un procedimiento de cooperación entre los Estados miembros en los supuestos de tratamientos denominados transfronterizos, con la participación de todas las autoridades implicadas, pero no regula el modo en que el Derecho interno de los

[250] «BOE» núm. 183, de 30 de julio de 2018, páginas 76249 a 76257
https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751

Estados habrá de verse afectado como consecuencia de los trámites previstos en la propia norma europea para estos procedimientos.

Todos esos aspectos determinaron la necesidad de adaptar transitoriamente el marco normativo interno al Reglamento General de protección de datos, tarea que el Consejo de Ministros impulsó mediante la aprobación, en su sesión de 10 de noviembre de 2017, de un proyecto de Ley Orgánica, remitido a las Cortes Generales, que se aprobó y publicó en el BOE en el mes de diciembre de 2018.

Sin perjuicio de lo anterior, en relación con aquellos aspectos que no son objeto de reserva de Ley Orgánica, y en tanto se procedía a la completa revisión del marco normativo, se aprobó con carácter urgente la norma con rango de ley objeto del presente epígrafe, y cuyo objeto era permitir la adaptación temporal del Derecho español al Reglamento General de protección de datos de la Unión Europea. Ciñéndose, no obstante, "a la adecuación de nuestro ordenamiento al reglamento europeo en aquellos aspectos concretos que, sin rango orgánico, no admiten demora y debe entenderse sin perjuicio de la necesidad de una legislación orgánica de protección de datos que procure la plena adaptación de la normativa interna a los estándares fijados en la materia por la Unión Europea a través de una disposición directamente aplicable"[251].

Esa norma se aprobó a finales del mes de julio del año 2018, y se denominó "*Real Decreto-ley de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos*"[252].

El contenido de ese Real Decreto-ley está bien resumido en su preámbulo[253], que expone como esa norma "comprende catorce artículos estructurados en tres

[251] Último párrafo del apartado I del preámbulo.
[252] Misma referencia que 250.
[253] Apartado II del preámbulo.

capítulos, dos disposiciones adicionales, dos transitorias, una derogatoria y una final", afectando su contenido únicamente, "a cuestiones cuya inmediata incorporación al Derecho interno resulta imprescindible para la adecuada aplicación en España del Reglamento General de protección de datos y que no están excluidas del ámbito del legislador de urgencia por el artículo 86 de la Constitución Española".

El Capítulo I, atendería "a la necesidad de identificar al personal competente para el ejercicio de los poderes de investigación que el Reglamento General de protección de datos otorga en su artículo 58.1 a las autoridades de control". Ello exige que el Derecho interno "regule el modo en que podrán ejercerse dichos poderes, qué personas ejercerán la actividad de investigación e inspección y en qué consistirán esas atribuciones expresamente establecidas en el reglamento europeo desde el punto de vista del ordenamiento español". Asimismo, y en aplicación del artículo 62.3 del Reglamento General de protección de datos, "es preciso determinar el régimen aplicable al personal de las autoridades de supervisión de otros Estados miembros que participen en actuaciones conjuntas de investigación".

El Capítulo II "articula el novedoso régimen sancionador establecido en el Reglamento General de protección de datos", "reemplazando los tipos infractores actualmente contenidos en la Ley Orgánica 15/1999 por la remisión a los que están establecidos en los apartados 4, 5 y 6 del artículo 83 de dicho reglamento, lo que resulta de todo punto necesario". Además, "existen dos cuestiones sobre las que es ineludible la adopción de disposiciones por el Derecho interno que garanticen la efectividad de este régimen sancionador y la seguridad jurídica en su aplicación". "La primera se refiere a la necesaria delimitación de los sujetos que pudieran incurrir en la responsabilidad derivada de la aplicación de dicho régimen sancionador". "La segunda reviste aún mayor importancia y se refiere a la necesidad de determinar los plazos de prescripción de las infracciones y sanciones previstas en la norma europea".

El tercer y último capítulo (Capítulo III), "contiene la regulación del procedimiento en caso de que exista una posible vulneración del Reglamento General de protección de datos". En este punto, es preciso tener en cuenta que el reglamento distingue en la práctica tres tipos de tratamientos a los que aplicaría distintas normas procedimentales: los tratamientos transfronterizos, definidos por el artículo 4.23 del Reglamento General de protección de datos, los transfronterizos con relevancia local en un Estado miembro, a los que se refiere el artículo 56 del mismo, y aquéllos que tendrían la condición de exclusivamente nacionales, entre los que figuran en todo caso los previstos en el artículo 55 de la norma europea. El reglamento europeo prevé una serie de trámites específicos para los dos primeros supuestos entre los que se encuentran los necesarios para determinar la competencia de la autoridad de control principal, así como los que permiten la adopción de una decisión consensuada entre las autoridades principal e interesadas en el procedimiento. En estos casos la regulación europea establece la obligación de que la autoridad principal someta los distintos proyectos de decisión a las restantes autoridades, que dispondrán de plazos tasados para la emisión de «observaciones pertinentes motivadas», y previéndose el sometimiento de la resolución al Comité Europeo de Protección de Datos en caso de no alcanzarse un acuerdo entre todas ellas.

Por último, en cumplimiento del artículo 68.4 del Reglamento General de protección de datos[254], la disposición adicional primera "designa como representante de España en el Comité Europeo a la Agencia Española de Protección de Datos, que informará a las autoridades autonómicas acerca de las decisiones adoptadas en dicho organismo de la Unión y recabará su parecer cuando se trate de materias de su competencia". Por su parte, la disposición adicional segunda "contiene previsiones en lo relativo a la publicidad de las resoluciones de la Agencia Española de Protección de Datos, con el fin de garantizar la transparencia de su actuación, ante el nuevo marco procedimental configurado por el Reglamento General de protección de datos" [255].

[254] Regula la composición y características del Comité Europeo de Protección de Datos.
[255] Exposición de motivos del RD-ley objeto de análisis.

La disposición final única de esa norma dispone que "el presente real decreto-ley entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado»"[256] y lo estará de forma transitoria "hasta la vigencia de la nueva legislación orgánica de protección de datos que tenga por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones".

Fue derogado de forma expresa con la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* (numeral segundo de su disposición derogatoria única), a la cuya tramitación y contenido específico dedicaremos el epígrafe que sigue.

5.9. La nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: el reconocimiento positivo del derecho al olvido digital en la legislación española

5.9.1 Fase de tramitación del Proyecto de Ley Orgánica

El Proyecto de nueva *Ley Orgánica de Protección de datos de carácter personal* se presentó en el Congreso de los diputados el día 14/11/2017, siendo calificado el 21/11/2017. La Comisión competente para conocer ese dosier fue la Comisión de Justicia.

[256] Su publicación en el BOE» núm. 183, de 30 de julio de 2018, determina su entrada en vigor el 31 de julio de 2018.

Con anterioridad a esa presentación, y según expuso en el Congreso de los Diputados el propio Ministro de Justicia, CATALÁ POLO[257] el día 15/2/2018, "el primer borrador de este proyecto fue elaborado por la Comisión General de Codificación, a través de una ponencia creada *ad hoc* para esta materia, dentro de la sección de derecho público". "Ponencia que mantuvo reuniones con la directora de la Agencia Vasca de Protección de Datos y con la directora de la Autoridad Catalana los días 6 de febrero y 10 de marzo de 2017". Así mismo, el proyecto recibió informes de distintos departamentos ministeriales, del Consejo Fiscal, del Consejo General del Poder Judicial y de las autoridades de protección de datos, y hasta un total de setenta informes de la sociedad civil en el trámite de información pública.

Por su parte, tanto la Agencia Española de Protección de Datos, como la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, elaboraron sus correspondientes informes, incorporándose al texto la mayor parte de las observaciones formuladas por esos organismos.

También se trabajó de forma estrecha con la Comisión Europea, a través de la comisaria de Justicia, Consumo e Igualdad de Género, que también formuló observaciones al texto que le fue remitido para su consideración. Finalmente, el Consejo de Estado expresó en su Dictamen un juicio favorable al conjunto del anteproyecto, concluyendo que: "nueva legislación representará un paso positivo en el tratamiento normativo de la materia a la que se ha enfrentado. El resultado es un texto de buena factura y de elevado nivel técnico".

Desde el 14 de diciembre de 2017 y hasta el 3 de abril de 2018 se articularon plazos sucesivos o ampliados para la presentación de enmiendas. Tras la correspondiente

[257] Diario de Sesiones del Congreso de los Diputados; Año 2018 XII Legislatura Núm. 104, Sesión plenaria núm. 99, celebrada el jueves, 15 de febrero de 2018
http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28DSCD-12-PL-104.CODI.%29#(P%C3%A1gina28)

tramitación Parlamentaria[258], la propuesta fue aprobada por unanimidad en el Pleno del Congreso de los diputados el pasado 18 de octubre de 2018, pasando el trámite legislativo al Senado[259], que lo aprobó de forma definitiva en el mes de noviembre de 2018.

5.9.2 Contenido de la Ley Orgánica

El contenido esa Ley Orgánica es el que sigue[260]: consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

En el título I se regulan las disposiciones generales (objeto de la ley y ámbito de aplicación), estableciendo para esa norma un doble objetivo: lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento General de protección de datos, y completar sus disposiciones, garantizando asimismo los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución".

---

[258] La iniciativa ha seguido la siguiente tramitación parlamentaria: Comisión de Justicia Publicación desde 21/11/2017 hasta 24/11/2017
Comisión de Justicia Enmiendas desde 24/11/2017 hasta 04/04/2018
Comisión de Justicia Mesa - Calificación desde 07/02/2018 hasta 08/02/2018
Comisión de Justicia Debate de totalidad desde 08/02/2018 hasta 15/02/2018
Comisión de Justicia Informe desde 04/04/2018 hasta 26/09/2018
Comisión de Justicia Dictamen desde 26/09/2018 hasta 10/10/2018
Pleno Aprobación desde 10/10/2018

[259] Respecto de la aludida tramitación parlamentaria, pueden consultarse en el BOCG los siguientes textos:

- Texto íntegro de la iniciativa: BOCG. Congreso de los Diputados Núm. A-13-1 de 24/11/2017 Pág.: 1
- Enmiendas e índice de enmiendas al articulado: BOCG. Congreso de los Diputados Núm. A-13-2 de 18/04/2018 Pág.: 1
- Informe de la Ponencia: BOCG. Congreso de los Diputados Núm. A-13-3 de 09/10/2018 Pág.: 1

[260] https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Como novedad, se incluye en ese título la regulación de los datos referidos a las personas fallecidas, disponiendo que sus herederos puedan acceder a los mismos, así como solicitar su rectificación y supresión.

El título II, "Principios de protección de datos", regula los principios de exactitud de los datos, deber de confidencialidad, tratamiento basado en el consentimiento del afectado, régimen del consentimiento de los menores de edad, tratamiento por obligación legal, interés público o ejercicio de los poderes públicos, así como las categorías especiales de datos y tratamiento de datos de naturaleza penal.

El título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, "que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada "información por capas" ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las "cookies"), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información".

En el título IV se recogen "Disposiciones aplicables a tratamientos concretos", incorporando una serie de supuestos respecto de los que el legislador establece una presunción iuris tantum de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1 e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general.

El título V se refiere al responsable y al encargado del tratamiento, reflejando el viraje del Reglamento (UE) 2016/679 a un sistema que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan.

El título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se ha de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la Ley Orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, *de Régimen Jurídico del Sector Público*, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El título VIII regula el "Procedimientos en caso de posible vulneración de la normativa de protección de datos". El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de "ventanilla única" en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la

tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

El título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la Ley Orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento General de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea.

Finalmente, el título X de esta Ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet[261]. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

[261] Sobre protección de menores y redes sociales, ver: MORILLA FERNÁNDEZ, M.: "La protección jurídica del menor ante las redes sociales", en BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador): *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras".

5.9.3 Reconocimiento positivo del Derecho al olvido digital en el ordenamiento español

Ya hemos expuesto brevemente como dentro del título X del texto definitivo de la *Ley Orgánica de protección de datos de carácter personal* se acomete la tarea de reconocer y garantizar un elenco de "derechos digitales de los ciudadanos", entre los cuales se reconoce, por vez primera en nuestro ordenamiento jurídico español, el derecho al olvido.

En particular, respecto de este derecho, son dos los artículos de la Ley Orgánica que abordan su regulación, el 93 y el 94, rubricados respectivamente "Derecho al olvido en búsquedas de Internet" y "Derecho al olvido en servicios de redes sociales y servicios equivalentes".

La redacción de esos preceptos es la que sigue:

> ***"Artículo 93. Derecho al olvido en búsquedas de Internet.***
>
> *1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como*

tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho".

Por su parte, el artículo 94 establece lo siguiente:

"Artículo 94. Derecho al olvido en servicios de redes sociales y servicios equivalentes.

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2."

Esto es, desde la aprobación definitiva del texto, publicación y entrada en vigor del mismo en diciembre de 2018, España es uno de los primeros países que ha reconocido de forma positiva y expresa en su normativa interna el "derecho al olvido digital", tanto desde la perspectiva del derecho a no ser indexado por los motores de búsqueda cuando la información que esa búsqueda arroje sea inexacta, inadecuada o impertinente, o hubiera adquirido esa condición por el paso del tiempo; como desde la perspectiva del derecho a que los datos de una persona sean suprimidos de los servicios de redes sociales (u otros equivalentes de la sociedad de la información), a su sola solicitud.

El texto aprobado amplía el ámbito del derecho al olvido o a la supresión de los resultados de las búsquedas de los motores efectuadas empleando como comandos de búsqueda el nombre y apellidos de una persona física determinada en aplicación de la jurisprudencia comunitaria "Google", a la solicitud de borrado de datos de redes sociales u otros servicios análogos, yendo más allá de las previsiones de la propia Sentencia del TJUE, pero dando así respuesta a la inquietud de muchos particulares

quienes se habrían quejado sobre estas prácticas tanto ante la AEPD como ante las Instituciones europeas, y anticipando una respuesta a este tipo de situaciones.

Destaca asimismo que la protección de los interesados es aún mayor en el caso de que los datos fueran facilitados a la red social cuando los mismos eran aún menores de edad. En cuyo caso "el prestador deberá proceder sin dilación a su supresión por su simple solicitud", en los mismos términos que lo hace la *California minor erase Law*[262], a la que aludiremos en el siguiente Capítulo de este trabajo, dedicado al derecho comparado[263].

5.9.4 Sentencia 76/2019, de 22 de mayo de 2019, del Pleno del Tribunal Constitucional dictada en el Recurso de inconstitucionalidad 1405-2019, interpuesto por el Defensor del Pueblo respecto del apartado primero del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del régimen electoral general, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales

Finalizamos el presente Capítulo mencionando la reciente y relevante Sentencia del Pleno del Tribunal Constitucional, de 22 de mayo de 2019. En esa Resolución judicial, ese Alto Tribunal declaró, por unanimidad, contrario a la Constitución y nulo el apartado 1 del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, *del Régimen Electoral General*, incorporado por la Ley Orgánica 3/2018, de 5 de diciembre, *de protección de datos personales y garantía de los derechos digitales*.

A través del apartado 2º de su disposición final tercera, esa LO modificaba la de Régimen electoral general, en los siguientes términos:

[262] California Senate Bill No. 568: *Privacy Rights for California Minors in the Digital World* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
[263] Capítulo 6

"Disposición final tercera. Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue

Uno. […]

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

«Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.

1. La recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales se encontrará amparada en el interés público únicamente cuando se ofrezcan garantías adecuadas.

2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.

3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.

4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

La reforma legislativa permitía a los partidos políticos recoger y tratar datos personales relativos a las opiniones políticas de los ciudadanos.

La Sentencia, cuyo ponente fue el Magistrado Cándido Conde-Pumpido, estimó el recurso de inconstitucionalidad presentado por el Defensor del Pueblo el pasado 5 de marzo de 2019, y declaró contrario a la Constitución y nulo ese apartado 1 del art. 58 bis de la Ley Orgánica 5/1985, de 19 de junio, d*el régimen electoral general*, incorporado por la disposición final tercera, apartado dos, de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Estima con buen criterio nuestro Tribunal Constitucional que la ley "no ha identificado la finalidad de la injerencia para cuya realización se habilita a los partidos políticos, ni ha delimitado los presupuestos ni las condiciones de esa injerencia, ni ha establecido las garantías adecuadas que para la debida protección del derecho fundamental a la protección de datos personales reclama nuestra doctrina, por lo que se refiere a la recopilación de datos personales relativos a las opiniones políticas por los partidos políticos en el marco de sus actividades electorales". Y que por tales motivos, "se han producido tres vulneraciones del artículo 18.4 CE en conexión con el artículo 53.1 CE, autónomas e independientes entre sí, todas ellas vinculadas a la insuficiencia de la ley y que solo el legislador puede remediar", y "redundando las tres en la infracción del mandato de preservación del contenido esencial del derecho fundamental que impone el artículo 53.1 CE, en la medida en que, por una parte, la insuficiente adecuación de la norma legal impugnada a los requerimientos de certeza crea, para todos aquellos a los que recopilación de datos personales pudiera aplicarse, un peligro, en el que reside precisamente dicha vulneración y, por otra parte, la indeterminación de la finalidad del tratamiento y la inexistencia de «garantías adecuadas» o las «mínimas exigibles a la Ley» constituyen en sí mismas injerencias en

el derecho fundamental de gravedad similar a la que causaría una intromisión directa en su contenido nuclear".

No podemos sino compartir el criterio expresado por el Tribunal Constitucional, que ha sido aplaudido por el conjunto de la sociedad española, y que evidencia los peligros que la portilla abierta a través de esa disposición final tercera de la Ley Orgánica 3/2018 suponía para los ciudadanos, quienes veían seriamente amenazado su poder de disposición y control sobre sus propios datos personales, en una materia tan sensible como lo es la relativa a las opiniones políticas, los cuales, por su vinculación con otros derechos y libertades, como la ideológica (artículo 16.1 CE) y las de expresión y comunicación [artículo 20.1.a) y d) CE], así como el principio de igualdad (artículo 14 CE), pertenecen a la categoría de datos especialmente protegidos.

CAPÍTULO 6

EL DERECHO AL OLVIDO DIGITAL EN LAS RESOLUCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y EN DERECHO COMPARADO.

SUMARIO: 6.1. GENERAL; 6.2 LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y SU ESTATUTO; 6.3. EXPEDIENTES DE TUTELA DE DERECHOS ANTE LA AEPD EN MATERIA DE DERECHO AL OLVIDO DIGITAL (EN 2019); 6.4. LA FUNCIÓN REVISORA DE LA SALA DE LO CONTENCIOSO-ADMINISTRATIVO DE LA AUDIENCIA NACIONAL; 6.5. DERECHO AL OLVIDO EN LOS PAÍSES DE NUESTRO ENTORNO COMUNITARIO; 6.5.1 FRANCIA; A) EL DERECHO DE DESINDEXACIÓN EN FRANCIA; B) LA CUESTIÓN RELATIVA AL ALCANCE TERRITORIAL DEL DERECHO A LA DESINDEXACIÓN; 6.5.2 ITALIA; 6.5.3 ALEMANIA; 6.5.4 BÉLGICA; 6.5.5 SUECIA; 6.6.6 REINO UNIDO; 6.6. DERECHO AL OLVIDO DIGITAL EN DERECHO COMPARADO: REPERCUSIONES DE LA SENTENCIA GOOGLE EN PAÍSES NO COMUNITARIOS; 6.6.1 EE.UU.; 6.6.2 CANADÁ; 6.6.3 CENTROAMÉRICA Y AMÉRICA DEL SUR; A) PAÍSES QUE RECONOCEN EXPRESAMENTE EL DERECHO AL OLVIDO EN SUS LEGISLACIONES; A.1. COSTA RICA; A.2. NICARAGUA; A.3. URUGUAY; B) PAÍSES QUE HAN RECONOCIDO EL DERECHO AL OLVIDO EN LA JURISPRUDENCIA; B.1. CHILE; B.2. COLOMBIA; B.3 PERÚ; B.4 ARGENTINA; B.5 PANAMÁ; 6.6.4 RUSIA; 6.6.6 CHINA; 6.6.7 AUSTRALIA

6.1 General

Resulta indiscutible el papel de la Agencia Española de Protección de Datos[264] tanto en la tramitación nacional del procedimiento *Costeja vs. Google* como en el sentido de la Sentencia del TJUE, *Google vs. España*[265]. Las tesis de la AEPD respecto de ese particular fueron plenamente asumidas por el Tribunal de Justicia de la Unión Europea en su histórica sentencia, en la que se daba respuesta a la cuestión prejudicial planteada en 2012 por la Audiencia Nacional.

Que duda cabe de que el sentido de esa Sentencia ha tenido un importantísimo impacto en la evolución de las reclamaciones recibidas por la Agencia desde el inicio de su actividad, hace este año (2019) veinticinco (desde 1994), y el perfil de las mismas.

---

[264] https://www.aepd.es/

[265] http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=7523737

Así, se tramitaron 81 reclamaciones en 1994, frente a las 13.000 recibidas en 2018. En aquellos años, las denuncias y tutelas de derecho presentadas por los ciudadanos ya mostraban que sus preocupaciones giraban en torno a aspectos relacionados con solvencia, crédito y morosidad y publicidad directa.

En 2018, la agencia recibió 1.784 reclamaciones sobre el ejercicio de todos los derechos de protección de datos -acceso, rectificación o cancelación-[266]. De ellas, casi 200 (191) corresponden a reclamaciones por derecho al olvido. La proporción estimadas/desestimadas de estas 191 tutelas/reclamaciones es prácticamente de un 50%. En cuanto a las entidades reclamadas, Google y sus servicios aglutinan 125 de las 191 (65%), 18 a medios de comunicación (9%), 14 a otros buscadores de Internet (7%), 13 corresponden a Administraciones Públicas y boletines (6%), cifras que se completan con un apartado de peticiones a otras entidades[267].

Consultados datos de la propia Google a agosto de 2019 (ya mencionados en el apartado 2º del Capítulo 3 del presente trabajo) desde el dictado de esa Sentencia (2014) el buscador ha recibido más de 800.000 solicitudes de desindexación (834.733)[268], que afectaban a 3.281.701 URL, de las que ha suprimido 1.199.955 –el 44,5% de las peticiones–. De todas estas, el 88,6% las habían promovido personas particulares; el resto correspondían a menores de edad, entidades corporativas, políticos y personas con cargo o relevancia pública. De esas más de 800.000 solicitudes, 79.710 se realizaron desde España, e incumbían a 261.125 URL[269]. De esas solicitudes formuladas en España, el buscador ha suprimido 81.813 enlaces, el 37,9%.

[266] https://www.aepd.es/media/memorias/memoria-AEPD-2018.pdf
[267] Datos tomados de: https://www.aepd.es/prensa/2019-05-21.html
[268] https://transparencyreport.google.com/eu-privacy/overview, a 17/8/2019.
[269] https://transparencyreport.google.com/eu-privacy/overview?requests_over_time=country:ES&lu=requests_over_time a 17/8/2019

En la primera parte del presente Capítulo ahondaremos en la figura de la Agencia Española de Protección de Datos, y analizaremos el contenido de algunas de esas resoluciones, para concluir, como tras el dictado de la *Sentencia Google* la Agencia Española de Protección de Datos ha primado, en la práctica totalidad de los casos, el derecho al olvido digital frente a otros derechos (libertad de expresión e información), siempre y cuando entre la difusión de la noticia y la solicitud de desindexación haya transcurrido un lapso temporal suficiente.

6.2 La Agencia Española de Protección de Datos y su Estatuto

El título VI de la Ley Orgánica 5/1992, de 29 de octubre, *de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal*[270], configuró la Agencia de Protección de Datos como un ente independiente que debe garantizar el cumplimiento de las previsiones y mandatos establecidos en esa LORTAD.

Algunos aspectos de esa Agencia fueron objeto de regulación en esa misma norma que, no obstante, no agotó la materia, encomendando al Gobierno la regulación de la estructura orgánica y la aprobación del Estatuto de la Agencia de Protección de Datos.

Se procedió a cumplimentar ese doble mandato, integrando la estructura del ente en su Estatuto propio, mediante la aprobación del Real Decreto 428/1993, de 26 de marzo, *por el que se aprueba el Estatuto de la Agencia de Protección de Datos*[271], que continúa vigente en cuanto no se oponga a la recientemente aprobada Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales.*

[270] «BOE» núm. 262, de 31 de octubre de 1992, páginas 37037 a 37045 (9 págs.); https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189
[271] https://www.boe.es/eli/es/rd/1993/03/26/428/com

La Agencia Española de Protección de Datos se configura hoy como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, *de Régimen Jurídico del Sector Público*, actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, y se relaciona con el Gobierno a través del Ministerio de Justicia. Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la meritada Ley 40/2015, de 1 de octubre, *de Régimen Jurídico del Sector Público*[272], es «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Ejerce sus funciones por medio del Director, considerándose sus actos, actos de la Agencia. Los actos dictados por el Director en el ejercicio de las funciones públicas de la Agencia agotan la vía administrativa. Contra ellos se podrán interponer los recursos contencioso-administrativos que resulten procedentes.

La regulación original contenida en la LORTAD ha sido recientemente sustituida por la contenida en la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*, que dedica su título VII (artículos 44 a 56) a la Agencia Española de Protección de Datos en tanto que autoridad nacional de protección de datos en España.

Sus funciones y potestades se establecen en el art. 47 de la LO 3/2018, que dispone que "corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esa Ley Orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en sus artículos 57 y 58, las contenidas en esa LO y en sus disposiciones de desarrollo".

La AEPD desarrolla actividades de investigación, regulación a través de circulares y acción exterior. La AEPD también intervendrá en procedimientos en caso de posible

[272] «BOE» núm. 236, de 02/10/2015
https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566&p=20151002&tn=2

vulneración de la normativa de protección de datos, en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquélla investigue la existencia de una posible infracción de lo dispuesto en el mencionado Reglamento y en LO 3/2018.

6.3 Expedientes recientes de tutela de derechos sustanciados ante la AEPD en materia de derecho al olvido digital (en 2019)

Si tecleamos el término "olvido" en el buscador de resoluciones de la AEPD[273], la búsqueda arroja aproximadamente 350 resultados (exactamente 332), correspondientes a la franja temporal entre los años 2009 y 2019. De esos 332 expedientes, 233 corresponden a expedientes de tutela de derechos.

En el presente año 2019, y hasta el mes de agosto de 2019, se han dictado por esa Agencia Española de Protección de Datos nueve resoluciones en materia de derecho al olvido.

De esas nueve resoluciones, han sido íntegramente estimatorias tres, considerando la AEPD que las informaciones publicadas no podían entenderse amparadas en las libertades informativas considerando el tiempo de antigüedad de los hechos, que hacían quebrar el principio de calidad de los datos (son resoluciones estimatorias las siguientes: Resolución Nº: R/00301/2019, Expediente Nº: TD/00111/2019; Resolución Nº: R/00297/2019, Expediente Nº: TD/00109/2019; Resolución Nº: R/00204/2019, Expediente Nº: TD/00059/2019).

[273] https://www.aepd.es/resoluciones/

En otras tres ocasiones, la AEPD ha estimado parcialmente las reclamaciones formuladas por los solicitantes, entendiendo que la reclamación debía prosperar respecto de algunas de las URLs denunciadas pero no frente a todas (son Resoluciones estimatorias parciales, la Resolución Nº: R/00307/2019; Expediente Nº: TD/00103/2019; Resolución nº: R/00290/2019, Expediente Nº: TD/00106/2019; y la Resolución Nº: R/00091/2019, dictada en el expediente Nº: TD/00068/2019).

Finalmente, el sentido de las tres últimas resoluciones ha sido totalmente desestimatorio, al considerar la AEPD que, ponderados los derechos en conflicto, nos encontraríamos ante informaciones que relacionadas con funciones que los reclamantes realizaban en un determinado ámbito profesional y con conexiones importantes de carácter público, tratándose de informaciones publicadas en 2017 (y no obsoletas), encontrándonos ante un tratamiento que la AEPD considera legitimado, al no entenderse acreditado que "los datos publicados sean inexactos o han quedado obsoletos, procediendo la desestimación de esta reclamación". Es el caso de las tres siguientes Resoluciones desestimatorias: Resolución Nº: R/00218/2019, Expediente Nº: TD/00067/2019; Resolución Nº: R/00193/2019, Expediente Nº: TD/00028/2019; y resolución Nº: R/00146/2019, Expediente Nº: TD/00024/2019.

Ya hemos mencionado anteriormente como desde el dictado de la *Sentencia Google* la Agencia Española de Protección de Datos ha estimado casi en la totalidad de los procedimientos de tutela de derechos que se han sustanciado ante dicho organismo, primando el derecho fundamental al olvido digital de los reclamantes frente a otros derechos, y ello incluso en supuestos de informaciones publicadas solo con cuatro o cinco años de antigüedad respecto de la solicitud de desindexación. SORIANO GARCÍA[274] concluye que "la libertad de información ha encontrado desde ese

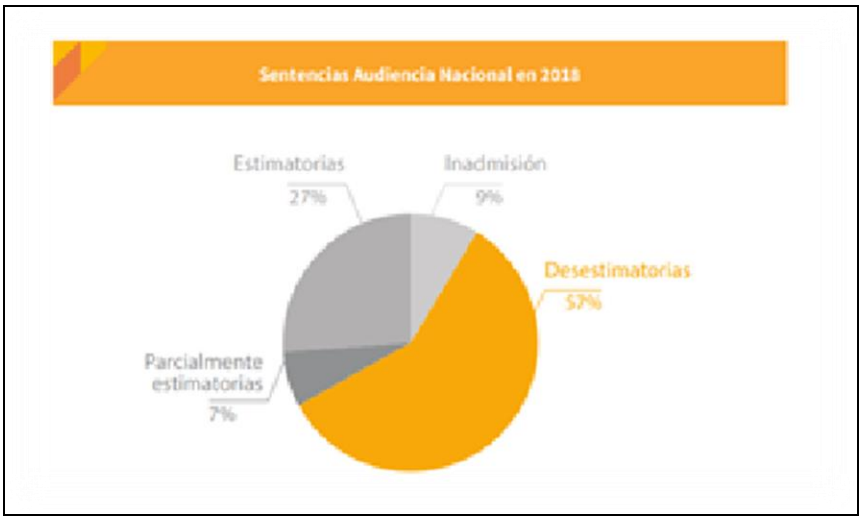
[274] SORIANO GARCÍA, J.E.: "Presente del derecho al olvido". *El Cronista del Estado Social y Democrático de Derecho*, ISSN 1889-0016, Nº. 78, 2018, págs. 4-21; ya citado

momento" una "nueva resistencia" "en la consolidación del derecho a la protección de datos".

No obstante, y como quiera que las Resoluciones del Director de la Agencia Española de Protección de Datos son recurribles ante la jurisdicción contenciosa, muchas de ellas han sido recurridas ante la Audiencia Nacional.

Consultados los datos de la Memorial Anual de la AEPD 2018 (pág. 104), muestran que el 52% de los procedimientos contenciosos interpuestos frente a esas resoluciones han sido desestimados y otro 9% adicional inadmitidos, siendo las Sentencias parcialmente estimatorias el 7%, y totalmente estimatorias el 27%.

Los aludidos resultados se muestran en el gráfico que reproducimos a continuación:



6.4. La función revisora de la Sala de lo contencioso-administrativo de la Audiencia Nacional

Ya hemos dicho como, desde el dictado de la *Sentencia Google*, la AEPD ha sido muy favorable a los reclamantes de olvido, estimando en la práctica totalidad de las ocasiones los expedientes de tutela del derecho al olvido digital instados ante dicho organismo, también en la práctica totalidad de las ocasiones frente a la mercantil Google LLC.

Sin embargo, la Sala de lo contencioso administrativo de la Audiencia Nacional ha revisado en no pocas ocasiones el criterio de la AEPD, que ha corregido, al estimar, por ejemplo:

1) **Sentencia de la Sala de lo contencioso-administrativo de la Audiencia Nacional (Sección 1ª), de 21 de junio de 2019**, dictada en el recurso núm: 106/2018[275], que revoca una imposición de desindexación de la AEPD a Google en el caso de dos noticias publicadas por el diario económico Alimarket en las que se informa de que el *Sr. Segundo*, como Director Ejecutivo de OKI Systems Ibérica, S.A., habría causado cuantiosas pérdidas económicas a esa sociedad que habrían ocasionado el cese de su actividad. Se refieren a información sobre actividad profesional del Sr. Segundo publicada en los años 2012 y 2013.a por los siguientes motivos:

    - "que dado el escaso tiempo transcurrido y el interés del público en acceder a la información publicada, han de prevalecer los derechos de libertad de expresión e información respecto del derecho a la protección de datos personales del afectado, al existir, por los expresados motivos, un interés legítimo de los internautas

[275] http://www.poderjudicial.es/search/indexAN.jsp?org=an&comunidad=13

potencialmente interesados en tener acceso a la información en cuestión (párrafo 81 de la STJUE de 13/05/2014)".

- Todo ello porque como razona la STS (1ª) 545/2015, de 15 de octubre, el llamado "derecho al olvido digital" que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos.

- Tampoco justifica que aquellos que se exponen a si mismo públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminado de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país.

2) En el mismo sentido se ha pronunciado esa Sala en otra **Sentencia también de 21 de junio de 2019 dictada en el recurso núm. 217/2018**[276], revocando la Resolución de la Agencia Española de Protección de Datos estimatoria del derecho al olvido digital del reclamante (un alcalde) frente a informaciones aparecidas en el diario El Faro de Vigo, que la Sala entiende prevalentes por revestir interés general.

[276] http://www.poderjudicial.es/search/indexAN.jsp?org=an&comunidad=13

3) Lo mismo ha sucedido con la **Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 21 de junio de 2019, en el recurso 215/2018**, según la cual debía primar también el derecho fundamental a la libre información y expresión en relación con determinados artículos periodísticos relativos al procedimiento penal seguido frente al Sr. Carlos Manuel por delitos de apropiación indebida o administración desleal, así como de la supuesta vinculación del Sr. Carlos Manuel con varios investigados y condenados por el Caso Gürtel.

4) O el de la **Sentencia de 16 de mayo de 2019, de la Sección 1ª de la Sala de lo contencioso administrativo de la Audiencia Nacional, en el recurso 609/2017**, en el que también se entiende prevalente el derecho a la libre información frente al derecho al olvido en un caso relativo a dos publicaciones en las que una multitud de afectados por el Sr. Augusto (reclamante), informan y vierten opiniones sobre las supuestas estafas que habría cometido como organizador del concurso "Juego de Talento", en el marco del festival de desarrollo de videojuegos CROMAfest, y, si bien el tono empleado en los comentarios pudiera parecer más o menos agrio, es indudable que es tolerable y entra dentro de los limites del derecho a la libertad de expresión.

5) Y el de la **Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 9 de mayo de 2019, en el recurso 491/2017**, según la cual serían también prevalentes los derechos del art. 20 CE frente al olvido digital ejercitado por D. Luis María frente a Google, y ordena el bloqueo de cincuenta y ocho url's que remiten a las sedes electrónicas del Senado, BOE, Gobierno del Principado de Asturias, Junta Electoral Central, Ministerio del Interior y otras en las que aparecen datos personales, en referencia a la publicación de listas electorales, en diversos medios, como candidato del partido político Democracia Nacional

Por el contrario, esa misma Sala de lo contencioso-administrativo de la Audiencia Nacional ha desestimado los recursos interpuestos frente a las siguientes resoluciones de la AEPD, cuyo criterio ha confirmado. Son ejemplos:

1) La **Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 22 de abril de 2019 en el recurso núm. 343/2017**, según la cual procede la exclusión de los datos personales del reclamante, al tratarse de datos obsoletos, al haber sido absuelto por la Sala de lo penal del TS del delito por el que le habían condenado y por lo que las urls reclamadas se asocian a su nombre. Debiendo prevalecer el derecho de la reclamante para que al realizar una consulta por su nombre y apellidos no se asocien las citadas urls, quedando satisfechos los derechos a la libertad de expresión e información al mantenerse los datos personales en las páginas de origen. Se trata en todos los casos de enlaces en los que aparecen los datos del Sr. Obdulio en noticias publicadas en medios de comunicación en el año 2006, en referencia a su detención por su implicación en el "caso Malaya" y su posterior condena (en primera instancia) a seis meses de prisión.

2) La **Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, en el recurso 528/2017, de 2 de abril de 2019**, desestimatoria del recurso interpuesto frente a la Resolución desestimatoria de la reclamación interpuesta ante la Agencia Española de Protección de Datos, al considerar esta que: "La resolución que se impugna, argumenta la denegación de la reclamación, en que la URL reclamada remite a una página web en la que se publica información del interesado consistente únicamente en su nombre y apellidos, y las funciones o puestos desempeñados en su actividad profesional de una empresa".

3) La **Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 26 de marzo de 2019 en el recurso núm. 468/2017**, que revoca y deja sin efecto la resolución de la Agencia Española de Protección de Datos por la que se obliga al portal Vanitatis a desindexar los datos del reclamante de una noticia, publicada en un diario digital, en la que se hace referencia al archivo de una querella que se interpuso contra el afectado por una supuesta estafa en la compraventa de unas viviendas, y que en dicha noticia se publica la fotografía de su hermano, jinete profesional y persona conocida.

Todos ellos son ejemplos de como en los cinco años que han transcurrido desde el dictado de la *Sentencia Google*, el balance entre los derechos del art. 18.1 y 18.4 CE y 20 CE, respecto del derecho al olvido digital, se está construyendo jurisprudencialmente, caso por caso, y como hasta la fecha venía haciéndose el balance entre esos mismos derechos en relación con el honor y la intimidad personal y familiar, en la búsqueda del deseado equilibrio entre privacidad e información.

6.5 Derecho al olvido en los países de nuestro entorno comunitario

La aplicación directa de lo dispuesto en el art. 17 del Reglamento General de protección de datos, determina que el derecho al olvido digital esté reconocido en todos los países de nuestro entorno comunitario. Si bien, ese derecho se ha implementado con matices en unos y otros Estados, destacando seguidamente y por su importancia, los asuntos de mayor relevancia resueltos en la materia en distintos países de la Unión Europea.

6.5.1 Francia:

a) El derecho de desindexación en Francia:

En aplicación del art. 17 del RGPD[277], la Comisión Nacional para la Informática y las Libertades[278] controla el cumplimiento de la obligación de desindexación en Francia.

En particular, la CNIL ha puesto a disposición del público a través de su portal de Internet un repositorio de todos los formularios puestos a disposición por los distintos motores de búsqueda en Internet[279] para llevar a cabo esa solicitud de desindexación a resultas de las obligaciones impuestas como consecuencia de la *Sentencia Google*. También ha desarrollado una herramienta que permite a los interesados verificar si su solicitud de desindexación ha sido atendida a través de tres navegadores distintos (Firefox[280], Chrome[281] y Opéra[282]), que permiten determinar si

---

[277] *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos) (Texto pertinente a efectos del EEE)*
https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32016R0679

[278] Creada en 1978 por la Ley n° 78-17 de 6 de enero 1978 relativa a la informática, los ficheros y las libertades, la CNIL es una autoridad administrativa independiente compuesta de un Consejo de 18 miembros y de un equipo de contratados laborales del Estado.
https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

[279]
BING https://www.bing.com/webmaster/tools/eu-privacy-request
GOOGLE
https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=636740646238090928-1600232400&hl=fr&rd=1
QWANT
https://about.qwant.com/wp-content/uploads/dlm_uploads/2017/02/dereferencement.pdf
YAHOO https://guce.oath.com/collectConsent?sessionId=3_cc-session_8aa54485-eef4-44fa-83c3-8de74a5a04c4&lang=&inline=false&jsVersion=null&experiment=null
IXQUICK

[280] FIREFOX
https://addons.mozilla.org/fr/firefox/addon/droit-au-d%C3%A9r%C3%A9f%C3%A9rencement/

[281] CHROME
https://chrome.google.com/webstore/detail/droit-au-d%C3%A9r%C3%A9f%C3%A9rencement/gpbababaddhddlmfhikljljamaikfghf

[282] ÓPERA
https://addons.opera.com/fr/extensions/details/droit-au-dereferencement/?display=fr

un sitio web aparece, o no, entre los resultados de un motor de búsqueda a partir de una búsqueda realizada por un nombre y apellidos.

b) La cuestión relativa al alcance territorial del derecho a la desindexación.

El 19 de julio de 2017[283], el Consejo de Estado francés elevó a la Corte de Justicia de la Unión Europea[284] una nueva cuestión prejudicial concerniente al derecho de desindexación o al derecho al olvido digital, y en particular, sobre la forma en la que, según la Corte de Justicia de la Unión Europea, debería interpretarse el alcance territorial de ese derecho[285].

El origen de esa nueva cuestión prejudicial fue una multa de 100.000 € impuesta a la sociedad Google Inc. mediante resolución de fecha de 10 de marzo de 2016, por haberse negado a acatar la Decisión de la Comisión Nacional de la informática y de las libertades (CNIL[286]), de 21 de mayo de 2015, que le requería para eliminar todos los resultados de una búsqueda efectuada bajo el nombre y apellidos de una persona en un determinado plazo. Google se negó a acatar el alcance de esa resolución, que imponía a la compañía la obligación de desindexar cualesquiera resultados (nombres de dominio) que arrojase el motor de búsqueda como resultados de esa búsqueda, y no solo las extensiones de dominio .fr o aquellas de los países integrantes de la UE. En el criterio de Google, la decisión del CNIL excede el ámbito de aplicación de la norma.

[283] CE, 19 juillet 2017, GOOGLE INC. N° 399922 http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC
[284] Publicada en el Diario Oficial de la Unión Europea el 16.10.2017
[285] http://www.conseil-etat.fr/Actualites/Communiques/Portee-territoriale-du-droit-au-dereferencement
[286] http://www.cil.cnrs.fr/CIL/spip.php?article2890

La mercantil Google Inc. solicitó ante el Consejo de Estado francés:

1°) que anulase la resolución n° 2016-054 de la Comisión Nacional de la Informática y las libertades (CNIL) de 10 de marzo de 2016;

2°) subsidiariamente, que elevase a la Corte de Justicia de la Unión Europea una cuestión prejudicial sobre la interpretación de los artículos 4 y 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

En el contexto de ese procedimiento, surgió la necesidad de elevar ante el TJUE esas cuestiones prejudiciales sobre la interpretación del alcance territorial de esa norma. Particularmente, las tres cuestiones prejudiciales planteadas fueron:

> *"La question de savoir si le « droit au déréférencement » tel qu'il a été consacré par la Cour de justice de l'Union européenne dans son arrêt du 13 mai 2014 sur le fondement des dispositions des articles 12, sous b), et 14, sous a), de la directive du 24 octobre 1995, doit être interprété en ce sens que l'exploitant d'un moteur de recherche est tenu, lorsqu'il fait droit à une demande de déréférencement, d'opérer ce déréférencement sur l'ensemble des noms de domaine de son moteur de telle sorte que les liens litigieux n'apparaissent plus quel que soit le lieu à partir duquel la recherche lancée sur le nom du demandeur est effectuée, y compris hors du champ d'application territorial de la directive du 24 octobre 1995, soulève une première difficulté sérieuse d'interprétation du droit de l'Union européenne*[287].
>
> *En cas de réponse négative à cette première question, la question de savoir si le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son*

[287] *La cuestión de si el "derecho de desindexación" consagrado en la Sentencia del Tribunal de Justicia de 13 de mayo de 2014 sobre la base de las disposiciones del artículo 12 (b) y 14 (a) de la directiva del 24 de octubre de 1995 debe interpretarse en el sentido de que el operador de un motor de búsqueda que acceder a una solicitud de desindexación, está obligado a realizarla en todos los nombres de dominio de ese motor de tal manera que los enlaces en disputa ya no aparezcan de ninguna manera, independientemente del lugar desde el que se realice la búsqueda lanzada con el nombre del solicitante, e incluso fuera del ámbito territorial de aplicación de la Directiva, planteando una primera y seria dificultad para interpretar el derecho de la Unión Europea.*

arrêt précité doit être interprété en ce sens que l'exploitant d'un moteur de recherche est seulement tenu, lorsqu'il fait droit à une demande de déréférencement, de supprimer les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir du nom du demandeur sur le nom de domaine correspondant à l'Etat où la demande est réputée avoir été effectuée ou, plus largement, sur les noms de domaine du moteur de recherche qui correspondent aux extensions nationales de ce moteur pour l'ensemble des Etats membres de l'Union européenne soulève une deuxième difficulté sérieuse d'interprétation du droit de l'Union européenne[288].

En outre, la question de savoir si, en complément de l'obligation évoquée au point précédent, le « droit au déréférencement » tel que consacré par la Cour de justice de l'Union européenne dans son arrêt précité doit être interprété en ce sens que l'exploitant d'un moteur de recherche faisant droit à une demande de déréférencement est tenu de supprimer, par la technique dite du « géo-blocage », depuis une adresse IP réputée localisée dans l'Etat de résidence du bénéficiaire du « droit au déréférencement », les liens litigieux des résultats affichés à la suite d'une recherche effectuée à partir de son nom, ou même, plus généralement depuis une adresse IP réputée localisée dans l'un des Etats-membres soumis à la directive du 24 octobre 1995, ce indépendamment du nom de domaine utilisé par l'internaute qui effectue la recherche, soulève une troisième difficulté sérieuse d'interprétation du droit de l'Union européenne[289].

[288] *En caso de respuesta negativa a esa primera pregunta, la cuestión sería si el «derecho a la desindexación» consagrado en la sentencia del Tribunal de Justicia de la Unión Europea precitada debe interpretarse en el sentido de que el operador de un motor de búsqueda tiene la obligación de desindexar todos los enlaces que se muestran como resultados de una búsqueda hecha a partir del nombre del solicitante en el Estado de la Unión Europea desde el que se realiza la solicitud o, en términos más generales, los nombres de dominio del motor de búsqueda que corresponden a las extensiones nacionales de este motor para todos los Estados miembros de la Unión Europea.*

[289] *Por otra parte, la cuestión de saber si como complemento a la obligación mencionada en el punto anterior, el "derecho de desindexación" consagrado por el Tribunal de Justicia de la Unión Europea en su sentencia, debe interpretarse en el sentido de que se requiere que el operador de un motor de búsqueda que accede a una solicitud de exclusión está obligado a eliminar esas referencias, mediante la técnica denominada "geo-bloqueo", desde las direcciones IP ubicadas en el Estado de residencia del beneficiario de ese "derecho a eliminar la referencia" o también desde cualquier otra IP situada en los países en los que se aplica la Directiva de 24 de octubre de 1995, con independencia del nombre de dominio utilizado por el usuario que realiza la búsqueda.*

Esas cuestiones[290] fueron resueltas en la reciente Sentencia de 24 de septiembre de 2019[291], habiéndose sustanciado el acto de la vista el 11 de septiembre de 2018 anterior[292]. En ese acto, los abogados de la CNIL argumentaron que los derechos de los ciudadanos europeos estaban en juego, siendo preciso que las conclusiones de la *Sentencia Google* se aplicasen universalmente porque, en caso contrario, la situación de la UE sería una mera burbuja que comprometería los derechos de los europeos. Los abogados de Google argumentaron, en cambio, que las pretensiones del Francia y la CNIL no podían acogerse, ya que ni los estándares de los derechos a la libre información/expresión ni los de la protección de datos son los mismos en todo el mundo ni los pronunciamientos de esa Sentencia pueden aplicarse más allá del ámbito de aplicación de la norma. La Comisión Europea apoyó los argumentos de Google, entendiendo que no es posible aplicar la norma más allá de las fronteras de la Unión[293]. También el Abogado General sostuvo esta interpretación en sus conclusiones, publicadas el 10 de enero de 2019 pasado[294].

La Sentencia, que se esperaba con mucha expectación, se dictó finalmente el pasado día 24 de septiembre de 2019[295] y, como era esperable, se inclinó en interpretar el

[290] http://curia.europa.eu/juris/fiche.jsf?id=C%3B507%3B17%3BRP%3B1%3BP%3B1%3BC2017%2F0507%2FP&oqp=&for=&mat=or&lgrec=es&jge=&td=%3BALL&jur=C%2CT%2CF&dates=&pcs=Oor&lg=&parties=google&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=es&avg=&cid=78124

[291] Sentencia del Tribunal de Justicia de la Unión Europea, Gran Sala, de 24 de septiembre de 2019, asunto C-507/2017 http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=6620230

[292] https://phys.org/news/2018-09-google-case-eu-globally.html

[293] SCHECHNER S., The Wall Street Journal, Sept. 11, 2018; EU Opposes France on Global 'Right to Be Forgotten', https://www.wsj.com/articles/eu-executive-arm-opposes-france-on-global-right-to-be-forgotten-1536685575

[294] http://curia.europa.eu/juris/document/document.jsf?text=&docid=209688&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1864979

[295] En esa misma fecha se ha dictado otra Sentencia del TJUE relativa a la interpretación que ha de hacerse del derecho al olvido digital y los motores de búsqueda, relativa a enlaces a páginas en las que se contiene artículos periodísticos de naturaleza penal (Asunto C-136/2017). El TJUE concluye que el balance deberá hacerse caso por caso, y que dependerá de las particulares características de cada supuesto que deba primar uno u otro derecho. En todo caso, estará obligado a estimar la solicitud de desindexación "cuando estos se refieran a una etapa anterior del procedimiento judicial de que se

derecho como lo hicieron la Comisión y el Abogado General. Esto es, entendiendo la norma en el sentido de que "cuando el gestor de un motor de búsqueda" (en este los responsables del buscador Google), "estime una solicitud de retirada de enlaces en virtud de estas disposiciones estará obligado a proceder a dicha retirada, no en todas las versiones de su motor, sino en las versiones de éste que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada".

Finalmente, el TJUE se ha decantado por una interpretación de la Directiva que no excede el ámbito territorial de aplicación de la norma, resolviendo de esta manera el conflicto planteado y acogiendo en su respuesta el criterio del buscador[296].

La cuestión de si cabía, o no, la aplicación global del derecho al olvido digital (saber si el reclamante tiene derecho a la desindexación en todos los buscadores nacionales o solo en aquel a partir del cual se hace la solicitud), era uno de los grandes retos a los que se enfrentaba este nuevo derecho en el corto plazo[297]. El sentido de la reciente Sentencia del Tribunal de Justicia tendrá probablemente una repercusión social, doctrinal y jurisprudencial también grande (quizás no tanto como la tuvo en su día la

trate y, habida cuenta del desarrollo de este, ya no se ajusten a la situación actual, en la medida en que se constate, en el marco de la comprobación de los motivos de interés público importantes a los que se refiere el artículo 8, apartado 4, de dicha Directiva que, a la luz del conjunto de circunstancias del caso concreto, los derechos fundamentales del interesado, garantizados por los artículos 7 y 8 de la Carta, prevalecen sobre los de los internautas potencialmente interesados, protegidos por el artículo 11 de la Carta".
http://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=9114099

[296] PELLICER, Ll. "La justicia europea da la razón a Google y limita el derecho al olvido a la UE", El PAÍS, 24.09.2019,
https://elpais.com/sociedad/2019/09/24/actualidad/1569314265_134650.html

[297] Ver nota 295.

Sentencia Google, pero si importante), por cuanto de esa interpretación del TJUE dependerá la forma en la que deba aplicarse posteriormente ese derecho al olvido digital por los responsables de desindexar los contenidos de ese pronunciamiento en adelante.

6.5.2 Italia:

En Italia, "*il diritto all'oblio*" tiene una larga tradición dogmática, que refleja ARTEMI RALLO en su obra "El derecho al olvido en Internet: Google vs. España"[298].

En particular, la Corte de Casación italiana se pronunció sobre el derecho al olvido mediante la Sentencia núm. 5525/2012, de 5 de abril de 2012[299], a través de la cual la Corte imponía a los medios digitales la obligación de establecer un sistema que permitiese conocer el desenlace de las noticias publicadas, como sucedía en el caso sometido a consulta, en el que el motor de búsqueda arrojaba resultados sobre el inicio de investigaciones penales pero no mostraba los posteriores resultados absolutorios. La Corte impuso al medio de comunicación digital -que no al buscador-, la obligación de establecer esos sistemas que permitieran rastrear la evolución favorable de las noticias incluidas en las hemerotecas.

Con posterioridad a la Sentencia del TJUE Google, el Tribunal de Roma se ha pronunciado sobre la cuestión del derecho al olvido en la Sentencia de la Sala de lo Civil, de 3 de diciembre de 2015, n. 23771. En ese caso, y precisamente en aplicación de los criterios interpretativos y condiciones establecidas por el TJUE en la aludida *Sentencia Google*, el Tribunal romano rechazó la reclamación de un particular, de profesión abogado, quien solicitaba la desindexación de los resultados de un motor

[298] Citado en 108.
[299] https://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Norme%20e%20Tributi/2012/04/corte-cassazione-sentenza-5525-2012.pdf

de búsqueda que le vinculaban con determinados asuntos penales ocurridos en 2012 y 2013 y sobre los que aún no existía condena. Respecto de los mismos, la Corte romana estimó prevalente el derecho fundamental a la información frente al derecho al olvido digital del reclamante[300].

6.5.3 Alemania

En Alemania, la Sentencia del TJUE Google ha tenido su reflejo en la del Tribunal Regional Superior de Colonia I-15 U 197/15[301], cuyo contenido analiza el Dr. ENRICO PEUKER de la Universidad de Berlín en su artículo: "The right to be forgotten in Germany"[302].

La reclamante fue, cinco años antes de interponer la demanda, directora de una empresa que gestionaba una página web de citas. El nombre de la reclamante como directora de esa empresa puede encontrarse en sitios web que contienen extractos de registros comerciales, así como posts de blogs anónimos en los que se denuncian prácticas comerciales abusivas por parte de esa empresa. Por todo ello, la reclamante planteó una acción por la que se obligase al gestor del motor de búsqueda a eliminar los links que llevasen a esos sitios web y blogs.

En primer lugar, la Corte dispuso -basándose en la Ley de protección de datos alemana- que la reclamante no tenía derecho a que se omitieran o borrasen los links en cuestión de la lista de resultados porque no había habido ninguna injerencia en sus derechos fundamentales.

---

300 Ver VESTO, A.: "La tutela dell'oblio tra intimità e condivisione senza filtri". *Rivista di dirito dei media, 2/2018*.
301 Higher Regional Court (Oberlandesgericht) Köln, I-15 U 197/15
302 Ver PEUKER, E.: "The Right to be forgotten in Germany". *Droit à l'oubli en Europe et au-delà: The Right To Be Forgotten in Europe and beyond*; https://blogdroiteuropeen.files.wordpress.com/2018/04/the-right-to-be-forgotten-in-europe-and-beyond-26-april.pdf

La circunstancia de que fuera la antigua directora de esa empresa es una circunstancia relativa a la "esfera social" de esa persona por lo que los casos de infracción de derechos fundamentales solo pueden suceder si causan graves efectos sobre los derechos de la personalidad, tales como la estigmatización, marginación social u otros de gravedad equivalente. Pero este no era el caso objeto del litigio: en el criterio del tribunal. La circunstancia de haber sido la reclamante antigua directora general de una compañía, determina la prevalencia de los derechos a las libertades informativas de los motores de búsqueda y el derecho a la libertad de expresión de los autores de los blogs.

Más aún, la Corte no consideró preciso modificar los criterios de las leyes civiles en Alemania a la luz del caso del TJUE *Google vs. España*, ya que sería preciso diferenciar: de una parte, que la información relativa a la reclamante no tiene, en este caso, dieciséis años de antigüedad; de otra, que la posición o las informaciones relativas a la reclamante no son aspectos vinculados a aspectos de su vida privada o íntima, como si pasaba en el asunto de Google España en la que los resultados arrojados reflejaban la existencia de una deuda con la Seguridad Social. Además, la información en cuestión provenía en el caso de Alemania de registros mercantiles públicos. Finalmente, considerando que el único sitio web de citas aún estaba funcionando y seguía acusado de prácticas comerciales desleales, existía un interés del público a tener información sobre esa persona, quien hace no tanto tiempo fue responsable de ellas.

Por el momento, esta Sentencia del Tribunal regional superior de Colonia es la única que ha tratado el asunto del TJUE desde la perspectiva del derecho alemán. Sin embargo, en palabras del DR. PEUKER en el artículo que citamos: "parece ejemplificar la posible estrategia para implementar la Sentencia del TJUE Google c. España"[303] por cuanto "los tribunales alemanes pueden incluir los pronunciamientos de la

[303] "it seems to exemplify a possible strategy of handling the ECJ's Google Spain ruling",

Sentencia Google dentro del elaborado principio de la protección de los derechos personalísimos"[304] y haciendo esto "respetar las disposiciones del TJUE en relación con el derecho al olvido" a la par que "interpretar la ley alemana de protección de datos y el derecho civil"[305].

6.5.4 Bélgica

En una resolución publicada recientemente[306], la Corte belga de Casación[307] confirmó la amplia interpretación del concepto del "derecho al olvido" que había realizado previamente la Corte de apelación de la ciudad de Lieja (Sentencia de la Corte de apelación de Lieja 2013/RG/393, 25 de septiembre de 2014[308]).

La Sentencia tuvo su origen en una reclamación formulada por un particular frente a un periódico belga por haberse negado a atender la solicitud de retirada de sus archivos de una noticia publicada en 1994 relativa a un accidente de tráfico en el que habría fallecido dos personas y en el que se vio envuelto el solicitante.

En ese contexto, la Corte de apelación decidió que el dato del nombre y apellidos del reclamante era prescindible en la información, cuya publicación, por el contrario, causaba un grave daño a su reputación. En consecuencia, ordenó al medio que procediera a anonimizar la versión online del periódico. En la motivación de esa decisión la Corte apeló al denominado "derecho al olvido" objeto del presente

[304] "German courts may fit the Google Spain ruling into the elaborated German concept of personal rights protection"
[305] "And in doing so, respect the ECJ's legal assessments with regard to the "right to be forgotten" while interpreting and applying German data protection and civil law".
[306] https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/
[307] https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/06/download_blob.pdf
[308] https://lex.be/fr/doc/be/jurisprudence-juridatlocationliege/juridatjuridictioncour-d-appel-arret-25-septembre-2014-bejc_2014092511_fr

estudio, y en particular a la *Sentencia Google* del TJUE a la que hemos aludido de forma reiterada. El periódico, disconforme con la decisión de la Corte de apelación de Lieja interpuso frente a la Sentencia recurso ante la Corte de casación.

En su Sentencia, la Corte de casación confirmó que la publicación de artículos en periódicos digitales podía ser interpretada como una nueva revelación de datos del pasado judicial de una persona, que potencialmente puede infringir su derecho individual al olvido.

En el balance efectuado entre los derechos en conflicto la Corte de Casación belga confirmó que la publicación online de un artículo no anonimizado relativo a un accidente de tráfico sucedido largo tiempo atrás podía causar perjuicio grave e injustificado a la persona citada, constituyendo una carga desproporcionada a soportar en relación con la libertad de información y expresión del medio de comunicación con el que se produce ese conflicto. Según la Corte de Casación, en el caso analizado debe primar el derecho a la intimidad del particular concernido sobre el derecho a la información del medio, motivo por el que confirmó la decisión de los tribunales de instancias inferiores que obligaban al periódico a eliminar todas las referencias a los datos que permitían la identificación del reclamante contenidos en esa noticia incluida en la hemeroteca online del medio.

6.5.5 Suecia

Según expone la Profesora de la Universidad de Södertörn, PATRICIA JONASON[309], con remisión a los datos contenidos en los informes de transparencia publicados por la propia Google, desde el dictado de la Sentencia Costeja, Google Inc. ha recibido 54.038 solicitudes de desindexado de urls suecas. De esas 54.038 solicitudes Google ha atendido el 43.7% y ha rechazado el resto. Esto es: Google ha rechazado acceder a las solicitudes de desindexación en un poco más de la mitad de los casos planteados.

Hasta el momento de la implementación del RGPD no existía en Suecia un derecho de desindexación, reconocido positivamente en una norma, por lo que son muy escasas las reclamaciones tanto ante la Autoridad sueca de protección de datos, como los que han llegado a los Tribunales como consecuencia de la negativa de Google de atender las solicitudes de borrado.

Respecto de estas últimas, la PROF. JONASON en el artículo que citamos recoge solo dos, y en uno de los cuales se alcanzó además un acuerdo extraprocesal, de tal forma que solo existe un caso judicial sobre el que los Tribunales suecos se hayan pronunciado en la materia.

En ese asunto, la Corte de primera instancia de Estocolmo fallo a favor de Google, en una Sentencia de 9 de mayo de 2016, en la que rechazó la eliminación de determinados links y condenó al reclamante a una importante suma en concepto de costas procesales (37.000 €).

El reclamante, el señor R.H., solicitó a la filial sueca de Google que retirase siete links que aparecían como resultados de búsqueda de Google en Suecia, de los que Google

[309] JONANSON, P.: "The digital right to be forgotten in Sweden: the theory and practice of privacy protection mechanisms in the face of referencing by search engines"
Droit à l'oubli en Europe et au-delà https://blogdroiteuropeen.files.wordpress.com/2018/04/the-right-to-be-forgotten-in-europe-and-beyond-26-april.pdf

accedió a retirar dos, pero mantuvo cinco, al considerar que contenían datos de la vida profesional del reclamante que tenían relevancia para la opinión pública. Al no obtener la respuesta esperada de Google, el actor reprodujo su solicitud ante los Tribunales de justicia. En particular el reclamante, que era gerente de una empresa de construcción, solicitaba la retirada de determinados artículos publicados entre 2010 y 2011 publicados en magazines vinculados al mundo inmobiliario que en su criterio contenían información ofensiva y desactualizada. También alegaba que esa publicación suponía el tratamiento inconsentido de sus datos de carácter personal, vulnerando la legislación sectorial de protección de datos. Además de la retirada de los links, exigía una indemnización de 1000 € y el pago de las costas del proceso.

Google alegó que la reclamación debía desestimarse, en primer lugar, porque la filial sueca de Google no podía entenderse responsable del tratamiento. También alegó la prevalencia del derecho de los usuarios a estar informados frente al derecho del reclamante a la protección de datos.

En su Sentencia, la Corte resuelve que, en el presente caso, y a pesar de que el medio no tuviera el consentimiento del reclamante para el tratamiento de sus datos, serían prevalentes los derechos a la libertad de información y expresión frente al derecho a la protección de datos de carácter personal invocado por el demandante. No en vano, el reclamante era consejero delegado de una compañía inmobiliaria, motivo por el que las informaciones denunciadas, que además se escribieron con fines periodísticos, se enmarcaban en el ámbito de su vida profesional y en su "rol en la vida pública", que no personal. Para alcanzar su veredicto la Corte también consideró la significativa importancia de la información publicada para el público, así como el hecho de ser informaciones relativamente recientes.

6.5.6 Reino Unido

Los dos primeros pronunciamientos sobre el derecho al olvido en el Tribunal Supremo de Inglaterra y Gales se produjeron en abril de 2018, fallando la Corte en uno de esos pronunciamientos a favor del interés del particular respecto de la eliminación de sus datos, y en cambio en el otro a favor de Google[310].

El ponente, Juez Warby de Londres, estimó la reclamación de un hombre de negocios que fue condenado por intercepción de las comunicaciones y que cumplió una sentencia de seis meses de prisión hace más de diez años. En cambio, rechazó las pretensiones de otro hombre que fue condenado a cuatro años de cárcel por falsa rendición de cuentas. Ambas personas habían reclamado de Google que eliminase los resultados de búsqueda que arrojaban los resultados sobre sus condenas. Google se negó y ambos recurrieron ante los Tribunales. En su decisión, Warby también consideró, en relación a la acción estimada, que los delitos por los que los reclamantes habían sido condenados no tenían implicaciones para los consumidores, clientes o inversores.

Al ser estos asuntos los primeros de una larga lista de reclamaciones, no se descarta que lleguen a causar, incluso, una revisión de las políticas de Google respecto de la desindexación de informaciones en Reino Unido.

310 https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case

6.6 Derecho al olvido digital en Derecho comparado: repercusiones de la Sentencia Google en países no comunitarios

El derecho al olvido digital no solo ha sido reconocido en la normativa sectorial comunitaria a través del artículo 17 del Reglamento Europeo de Protección de Datos, sino que ese derecho también ha tenido un reflejo positivo en las legislaciones de distintos Estados miembros de la Unión Europea y en la de Estados terceros.

En relación con estos últimos, expondremos seguidamente los desarrollos jurisprudenciales y legislativos más interesantes y recientes.

6.6.1 EE.UU

Es difícil imaginar la implantación del derecho al olvido digital en Estados Unidos por dos razones principales: la primera, la fortaleza de su Primera Enmienda a la Constitución, que impide la restricción legal de dos derechos fundamentales (que son la libertad religiosa y a la libertad de expresión) y que ha sido defendida de forma férrea por los Tribunales Estatales y por la Corte Suprema como uno de los pilares básicos del ordenamiento norteamericano.

Sobre el particular, cabe destacar las conclusiones alcanzadas por EUGENE VOLOKH[311] Profesor de Derecho de la Facultad de UCLA especializado en la materia, en un Estudio encomendado por Google y titulado "Google First Amendment Protection for Search Engines Results" y según el cual "los resultados de un buscador deberían ser considerados como una opinión basada en lo que dicho buscador considera más relevante para sus usuarios", y por tanto, estarían protegidos por la

[311] VOLOKH, E: "Google: First amendment protection for Search Engine search results", published version of a White Paper commissioned by Google, http://www2.law.ucla.edu/volokh/searchengine.pdf

Primera Enmienda de la Constitución de los Estados Unidos, que protege la libertad de expresión[312].

La segunda razón es la posición muy relevante que los gigantes de Internet (Google, Yahoo, Microsoft, Facebook, etc.) ostentan en el mercado norteamericano, la circunstancia de haber crecido de una manera tan espectacular precisamente por haber tenido que hacer frente a una regulación más bien escasa respecto de estas materias, y las dificultades que la implantación de derechos nuevos, como lo es el Derecho al olvido, podrían encontrar para su instalación efectiva.

No obstante lo anterior, y a resultas del fallo de la Sentencia del TJUE "Google", el 7 de julio de 2015[313] la organización de consumidores Consumer Watchdog[314], propuso ante la Comisión Federal de Comercio[315] una propuesta para implementar un concepto legal similar al derecho al olvido digital en los Estados Unidos. La asociación argumentó que la implementación de una idea así permitiría a los ciudadanos americanos recuperar la intimidad que habrían perdido como consecuencia de haber publicado determinada información en Internet.

En apoyo de la anterior iniciativa, una encuesta llevada a cabo por Adweek[316] concluyó que 9 de cada 10 norteamericanos querían que, de una u otra forma, el derecho al olvido digital se aplicase en los Estados Unidos. En 2015, un evento

[312] *"Google, Microsoft's Bing, and Yahoo! Search exercise editorial judgment about what constitutes useful information and convey that information—which is to say, they speak—to their users. In this respect, they are analogous to newspapers and book publishers that convey a wide range of information from news stories and selected columns by outside contributors to stock listings, movie listings, bestseller lists, and restaurant guides. And all of these speakers are shielded by the First Amendment, which blocks the government from dictating what is presented by the speakers or the manner in which it is presented".*
[313] https://www.minclaw.com/right-to-be-forgotten/
[314] http://www.consumerwatchdog.org/node/68111
[315] La Comisión Federal de Comercio (FTC, por su sigla en inglés) es responsable de asegurar que el mercado de consumo sea eficiente y no tenga restricciones. La Comisión hace cumplir las leyes federales de protección a los consumidores y las leyes de antimonopolio y competencia. https://gobierno.usa.gov/agencias-federales/comision-federal-de-comercio
[316] https://www.adweek.com/

organizado por Intelligence Squared US[317], un organizador de debates del estilo de Oxford, llevó a cabo un debate sobre si en Estados Unidos debería implementarse el derecho al olvido. El 56% de la audiencia de ese debate respondió que sí. Los escépticos con el fallo del Tribunal de Justicia de la Unión Europea y su implementación en los Estados Unidos se preguntaban, en línea con las anteriormente expuestas ideas del Profesor VOLOCK, si un derecho así podría sobrevivir en Estados Unidos, considerando la amplitud del contenido de la Primera Enmienda a la Constitución.

Sigue sin existir, hoy en día, una norma que formalmente reconozca el derecho al olvido digital en Estados Unidos. Ello sin perjuicio de que otras leyes protejan la privacidad y el derecho a la libertad de información/expresión de forma respectiva.

El esfuerzo más destacable por implantar en Estados Unidos una referencia legal expresa al derecho al olvido lo constituye la Ley nº A05323 del Estado de Nueva York[318], en tramitación ante la Asamblea de ese Estado desde el mes de febrero de 2017. Bajo la rúbrica: "An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act", la norma se dividiría en tres secciones, con el siguiente contenido:

- La sección primera exigiría a los motores de búsqueda que eliminen, previa solicitud del interesado, la información sobre un individuo que sea "inexacta", "irrelevante", "inadecuada" o "excesiva".

317 https://www.intelligencesquaredus.org/debates/us-should-adopt-right-be-forgotten-online
318 Senate Bill No. 568, *An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act* https://assembly.state.ny.us/leg/?default_fld=%0D%0A&leg_video=&bn=A05323&term=2017&Summary=Y&Actions=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y&Memo=Y&Text=Y

- La sección segunda prevé una acción para el resarcimiento de daños que se devengarían una vez transcurridos treinta días desde la recepción de la solicitud de retirada y en caso de no ser esa solicitud atendida por el buscador. En tal caso, por cada día que transcurra sin que la misma haya sido atendida se devengarían a favor del interesado doscientos cincuenta dólares.

- La Sección 3ª encomienda al Secretario de Estado hacerse cargo de las solicitudes, presentaciones, decisiones y sanciones relativas al derecho al olvido.

Esa norma está siendo objeto de tramitación ante la Asamblea del Estado de Nueva York.

No menos loables son los esfuerzos del estado de California para proteger a los menores de 18 años residentes en ese Estado solicitar de los servidores online, incluidas páginas web, aplicaciones móviles, redes sociales y otros servicios de Internet, la retirada de información personal, lo cual es posible a través de la *California Minor Eraser Law*[319], que entró en vigor el 1 de enero de 2015.

Adicionalmente, y en línea con lo anterior, la *Comisión Federal del Comercio*, vigila el cumplimiento de la *Children's Online Privacy Protection Rule* (COPPA)[320], norma a través de la cual se regula la captación de datos e información de menores en Internet.

[319] California Senate Bill No. 568: *Privacy Rights for California Minors in the Digital World* https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
[320] *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. 6501–6505; https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

6.6.2 Canadá

En Canadá no existe un derecho al olvido equivalente al existente en la legislación comunitaria. No obstante, a través del derecho de acceso a los datos personales y la obligación de las empresas de tener esos datos al día, la *Ley para la protección de la información personal y los documentos electrónicos*[321] confiere a ese derecho a la rectificación de datos personales.

En el asunto *globe24h.com*[322], el Tribunal Supremo Canadiense se ha pronunciado por primera vez sobre una solicitud de eliminación de datos y el derecho al olvido.

El sitio web *www.Globe24h.com* está albergado en un servidor situado físicamente en Rumanía. El sitio publica las resoluciones de los Tribunales canadienses pero, a deferencia de los sitios canadienes como *www.CanLII.org*, los resultados de Globe 24h son indexados por motores de búsqueda como Google. De tal manera, efectuando una búsqueda por el nombre y apellidos de una persona es posible acceder a resoluciones judiciales en las que aparece ese nombre. El Comisariado para la protección de la vida privada en Canadá, había recibido 38 quejas de personas relativas a la actividad de Globe 24h que se acumularon en el asunto del que conoció la Corte Federal. Los reclamantes alegan que las decisiones incluyen datos personales de naturaleza delicada y que su indexación por Google constituye una intromisión en su derecho fundamental a la vida privada.

Las páginas indexadas en Globe24h contienen datos personales que son exactos y verídicos, públicos y que pueden ser encontrados en otras páginas de Internet. No obstante, también generan perjuicio a los aludidos, en tanto que Google los indexa mientras que a las otras páginas no.

---

[321] *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5) http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[322] A.T. c. Globe24h.com, 2017 CF 114. https://www.canlii.org/fr/ca/cfpi/doc/2017/2017cf114/2017cf114.html

La Corte Suprema Federal Canadiense, en la Sentencia que analizamos, no consagra un derecho al olvido que pueda hacerse valer por los ciudadanos canadienses frente a Google, pero si determina que las páginas en las que aparecen sus datos personales contravienen la meritada *Ley canadiense para la protección de la información personal y los documentos electrónicos*. Una vía "más moderada, práctica y eficaz en el contexto en el que es dictada" en el criterio del autor Pierre-Luc Deziel[323], Profesor de la Universidad Laval, de Quebec.

6.6.3 Centroamérica y América del Sur

El derecho al olvido digital está expresamente reconocido en las legislaciones de Costa Rica (Artículo 11 D 37554/12), Nicaragua (Art. 10 L 787/12) y Uruguay (Ley núm. 18.331).

También ha sido reconocido jurisprudencialmente en países como Colombia, Perú, Argentina, Chile o Panamá, como pasamos a exponer.

[323] Le droit a l'oubli au Canada: L'affaire Globe 24h et le role du juge dans les requetes de dereférencement.
https://www.lemonde.fr/pixels/article/2019/09/24/le-droit-a-l-oubli-ne-s-applique-pas-au-monde-entier-tranche-la-justice-europeenne_6012818_4408996.html

a) Países que reconocen expresamente el derecho al olvido en sus legislaciones

a.1.) Costa Rica

El artículo 11 del Reglamento a la *Ley de Protección de la persona frente al tratamiento de sus datos personales*[324] de Costa Rica, en vigor desde el año 2013, reconoce el derecho al olvido digital en los siguientes términos:

> *"Artículo 11. Derecho al olvido. La conservación de los datos personales, que puedan afectar a su titular, no deberá exceder el plazo diez años, desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que establezca otro plazo o porque el acuerdo de las partes haya establecido un plazo menor. En caso de que sea necesaria su conservación, más allá del plazo estipulado, deberán ser desasociados los datos personales de su titular."*

La Agencia Nacional de Protección de Datos de los Habitantes de Costa Rica[325] ha reconocido este derecho en numerosas resoluciones, como lo son las que siguen, y en las que se ha obligado a la supresión de datos que, a pesar de haber sido exactos en su momento, han dejado de serlos como consecuencia del transcurso del tiempo. Son ejemplos: la Resolución NO. 03 de la PRODHAB, en el Expediente 074-12-2015-DEN, de 18.2.2016; Resolución NO. 04 de la PRODHAB, en el EXPEDIENTE: 029-06-2016-DEN, de 2.09.2016; Resolucion NO. 03 de la PRODHAB en el EXPEDIENTE: 040-06-2015-DEN, de 7.08.2015).

[324] Decreto Ejecutivo n.º 37554-JP; Publicado en el Alcance Digital n.° 42 a La Gaceta n.° 45 de 05 de marzo de 2013
[325] http://www.prodhab.go.cr/

a.2) Nicaragua

El artículo 10 de la Ley nº 787 *de Protección de datos personales* publicada en el Diario Oficial de Nicaragua el 29 de marzo de 2012[326], reconoce al titular de los datos el derecho a solicitar a las redes sociales, navegadores y servidores que supriman o cancelen datos que se encuentren en sus ficheros. Asimismo, se reconoce el derecho a que se cancelen aquellos datos obtenidos con motivo de una relación contractual, una vez esa relación llega a su fin.

a.3) Uruguay

En Uruguay[327], si bien el derecho al olvido carece de una regulación propia y específica, podría considerarse comprendido en el régimen general de protección de datos personales consagrado en la *Ley Nº 18.331* de 11 de agosto de 2008, modificativas y decretos reglamentarios.

El artículo 1º de esa *Ley Nº 18.331* dispone expresamente que "el derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República".

Esa norma, según resume SCHIAVI en su artículo "El Derecho al olvido y la protección de datos personales en Uruguay"[328], "consagra los derechos de los titulares de los datos, entre ellos, el derecho de toda persona para solicitar la rectificación,

[326] http://www.oas.org/es/sla/ddi/docs/N3%20Ley%20de%20Proteccion%20de%20Datos%20Personales.pdf
[327] SCHIAVI, P.: "El derecho al olvido y a la protección de datos personales en Uruguay"; *Revista de derecho de la Universidad de Montevideo*; Número 31 — AÑO 2017; http://revistaderecho.um.edu.uy/wp-content/uploads/2017/09/SCHIAVI-Pablo-El-derecho-al-olvido-y-a-la-proteccion-de-datos-personales-en-Uruguay.pdf
[328] http://revistaderecho.um.edu.uy/wp-content/uploads/2017/09/SCHIAVI-Pablo-El-derecho-al-olvido-y-a-la-proteccion-de-datos-personales-en-Uruguay.pdf

actualización, inclusión o supresión de datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular" (pág. 61).

b) Países que han reconocido el derecho al olvido a través de la jurisprudencia

b.1) Chile[329]

La Tercera Sala de la Corte Suprema de Chile proclamó por primera vez en ese país, mediante la Sentencia de fecha 21 de enero de 2016, el derecho al olvido digital, sobre el que a día de la fecha no existe aún una solución legislativa.

El derecho al olvido en esa Sentencia se conceptualiza con cita al autor español PERE SIMÓN CASTELLANO[330], a quien se cita de forma expresa en el considerando 5º de esa resolución, dando esa Corte Suprema un paso adelante al reconocer expresamente ese derecho en su sede de protección, partiendo de la base de que el uso legítimo de información y noticias puede volverse lesivo por el paso del tiempo y de manera sobrevenida.

En particular, la Corte Suprema de Chile estimó la reclamación efectuada por un Oficial de Carabineros de Chile acusado en el pasado de delito sexual frente al diario "El Mercurio", argumentando que esa información de su pasado les habría estigmatizado de por vida a él y su familia. El derecho al olvido se consagra a través de esa Sentencia en el ordenamiento chileno como un límite a la libertad de informar

329 http://www.derechoolvido.es/la-corte-suprema-de-chile-publica-una-sentencia-sobre-el-derecho-al-olvido/

330 SIMÓN CASTELLANO, P.: "El régimen constitucional del derecho al olvido en Internet", en "Neutralidad de la red y otros retos para el futuro de Internet. Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 11-12 de julio de 2011", Huygens Editorial, Barcelona, 2011, pp.391-406).

y a la libre circulación de información en la web, permitiendo reconocer que de manera sobrevenida ésta se puede volver lesiva de derechos fundamentales[331].

b.2) Colombia

Colombia es un referente mundial en el reconocimiento del derecho al olvido digital, por cuanto la Sentencia de la Corte Constitucional T-414/92[332] reconoció por primera vez este derecho, en una resolución dictada veintidós años antes de la Sentencia del TJUE.

En particular, la Corte Constitucional amparó a un ciudadano colombiano a quien la Asociación Bancaria le había negado en dos ocasiones su solicitud de ser excluido de una lista de morosos, y ello a pesar de estar la deuda prescrita.

La Corte estima que el reclamante (el "quejoso"), tenía "perfecto derecho" a reclamar la corrección de esos datos, y que al no hacerlo, y negársele el acceso al crédito, se le condenó socialmente.

Esa Sentencia manifiesta de forma expresa que "las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia, después de algún tiempo tales personas son titulares de un verdadero derecho al olvido" (fundamentación de la Corte D-5, el quinto epígrafe de esa Sentencia T-414/92, se titula: "La cárcel del alma y el derecho al olvido").

[331] RODRIGO PICA, F.: "El derecho fundamental al olvido en la web en el sistema constitucional chileno. Comentario a la sentencia de protección Rol Nº 22243-2015 de la Corte Suprema"; *Revista Estudios Constitucionales*, Año 14, Nº 1, 2016, pp. 309-318; ISSN 07180195 https://scielo.conicyt.cl/pdf/estconst/v14n1/art10.pdf

[332] Sentencia No. T-414/92, "Derecho a la intimidad personal y familiar/Derecho a la información", http://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm

La jurisprudencia más reciente[333], como la Sentencia de la Corte Constitucional T-040/13, aborda la cuestión de manera más restrictiva. En este sentido, la Corte Constitucional realizó un ejercicio de equilibrio entre los derechos de libertad de información, *habeas data*, buen nombre y honra, llegando a la conclusión de que no procede la eliminación de una referencia dañina a la parte demandante, a la que se conectaba con un cártel de la droga en una pieza periodística en Internet.

En este caso, la acción del demandante fue dirigida no solamente contra el periódico que publicó la noticia, sino también contra la filial colombiana de Google. No obstante, la Corte Constitucional determinó que el buscador no era responsable del contenido de las páginas que figuraban en su índice de búsqueda, centrando el foco en el medio en el que la noticia fue publicada. Finalmente, la Corte desestimó la pretensión de eliminar la referencia perjudicial, reconduciendo el caso al campo de la libertad de la información e instando al medio de prensa a publicar una rectificación que resarciera el daño causado.

La posterior Sentencia de la Corte Constitucional T-277/15 tiene un carácter similar, salvo que en este caso la acción iba dirigida solamente contra el periódico en cuestión, al que se le solicitaba que eliminase "de todos los motores de búsqueda disponibles y, específicamente, de Google.com cualquier información negativa en relación con la supuesta comisión del delito de trata de personas".

El análisis jurídico del fondo se basó en la contraposición de los derechos de buen nombre, honra y libertad de información. La Corte hace referencia a la STJUE C-131/12, pero finalmente decide apartarse de la misma al considerar que la solución alcanzada en ella no resulta idónea en el caso analizado por dos motivos. En primer lugar, la desindexación del artículo dañino no impediría el acceso al mismo mediante

[333] SANTOS VENTOSA, G: "Hacía el reconocimiento del derecho al olvido en Iberoamérica", noviembre 2016;
https://ecija.com/wp-content/uploads/2016/11/Derecho_al_olvido_Iberoamerica.pdf

un link directo. El segundo motivo se basa en garantizar, ante todo, el derecho de libertad de expresión (recogido en el mismo artículo de la Constitución Política colombiana que el derecho a la información) en conexión con el principio de neutralidad de Internet.

Finalmente, la Corte Constitucional instó al periódico demandado a que limitase la difusión de la noticia mediante el uso de herramientas técnicas como la modificación del archivo robots.txt y metatags, equilibrándose así los derechos de honra, buen nombre e información.

b.3) Perú

El derecho al olvido tampoco está reconocido positivamente en el ordenamiento jurídico del Perú. No obstante, como la *Ley de protección de datos peruana*[334] está claramente inspirada en la normativa española y comunitaria, fue cuestión de meses desde el dictado de la Sentencia del TJUE en el asunto Google que comenzasen a formularse en ese país reclamaciones tanto contra publicaciones en Internet como frente a buscadores ante la Dirección Nacional de Protección de Datos del Ministerio de Justicia[335].

Respecto de los motores de búsqueda, la Autoridad Nacional de Protección de Datos personales peruana ha sancionado, al menos en dos ocasiones a la entidad Google Inc. y Google Perú[336], con 30 y 35 UIT respectivamente, por no haber desindexado

[334] Ley nº 29733 de protección de datos personales de 3 de julio de 2011, http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf
[335] MORACHIMO, M.: "El discreto desembarco del Derecho al Olvido en Perú", https://revistaideele.com/ideele/content/el-discreto-desembarco-del-derecho-al-olvido-en-per%C3%BA
[336] Resolución Directoral N° 045-2015-JUS/DGPDP de fecha 30 de diciembre de 2015. Resolución Directoral N° 026-2016-JUS/DGPDP de fecha 11 de marzo de 2016 https://www.minjus.gob.pe/wp-content/uploads/2017/04/Cuadro-de-Sanciones-Impuestas-por-la-APDP-ABRIL-2017.pdf

los datos personales (nombre y apellidos) de una persona vinculada en el pasado a una causa penal que se sobreseyó, previo requerimiento de ésta. Las sanciones se imponen al amparo del art. 38, numeral 2 de la LPDP, que tipifica como sanción:

> *"c.) No atender, impedir u obstaculizar, en forma sistemática, el ejercicio de los derechos del titular de datos personales reconocidos en el título III, cuando legalmente proceda".*

Sobre las publicaciones, obligó al medio "El Peruano" a retirar en el plazo máximo de quince días los datos de los reclamantes cuyos nombres habían aparecido en dos resoluciones administrativas[337] dictadas con anterioridad.

b.4) Argentina

En Argentina, la Corte Suprema de Justicia de la Nación ha desestimado la existencia de un "derecho al olvido" en los términos en los que se ha reconocido en Europa en varias Sentencias, en las que ha reconocido la importancia de los buscadores, quienes entiende son "meros intermediarios", y a quienes exime de responsabilidad salvo supuestos excepcionales.

La primera resolución judicial en la que se tomó en consideración el alcance de la responsabilidad de los buscadores data de 2014 y es el asunto "Rodriguez"[338]. En

[337] Resolución Directoral N° 036-2015-JUS/DGPDP de fecha 24 de noviembre de 2015.
Resolución Directoral N° 09-2016-JUS/DGPDP de fecha 26 de enero de 2016.
https://www.minjus.gob.pe/wp-content/uploads/2017/04/Cuadro-de-Sanciones-Impuestas-por-la-APDP-ABRIL-2017.pdf

[338] http://www.telam.com.ar/notas/201410/83278-justicia-demanda-modelo-google-yahoo-derecho-al-olvido.html
Según recoge el diario Télam en una reseña de prensa publicada en aquella fecha: "En primera instancia, la demandante obtuvo fallo a favor contra Google, pero luego en la Cámara Civil redujeron la indemnización, de 100.000 a 50.000 pesos, en tanto que se rechazó la parte del reclamo relacionada con la supresión de las vinculaciones.
La sentencia de segunda instancia, apelada por ambas partes, llegó a la Corte Suprema de Justicia, donde los ministros ELENA HIGHTON, CARLOS FAYT y RAÚL ZAFFARONI votaron por rechazar la

aquella ocasión, una modelo demandó a los buscadores Yahoo y Google por mostrar entre sus resultados de búsqueda su imagen vinculada a sitios de contenido sexual. La modelo pedía un resarcimiento económico y la eliminación de su nombre, imágenes y fotografías de esos sitios de Internet, por el uso comercial y no autorizado de su imagen.

La Corte estimó que los buscadores "no tienen la obligación general de monitorear los contenidos que se suben a la red y que son proveídos por los responsables de cada una de las páginas de la red", no pueden ser condenados por lo que "no han creado". En el criterio de la mayoría, los buscadores de Internet son meros intermediarios a quienes no es posible exigirles responsabilidad de ninguna clase.

En la disidencia parcial se marcó la posibilidad de "solicitar la eliminación o bloqueo de enlaces que resulten claramente lesivos de derechos personalísimos" y también reclamar que "de acuerdo con la tecnología disponible, los buscadores adopten las medidas necesarias para prevenir futuros eventos dañosos".

El contenido del fallo del asunto Rodriguez se reprodujo en septiembre de 2017 en el asunto Gimbutas. Nuevamente una modelo reclamó la retirada de datos personales e imágenes suyas del buscador Google, desestimándose su solicitud por entender la Corte que los buscadores son meros intermediarios a quienes no les es exigible responsabilidad respecto del contenido de determinados sitios web.

pretensión y el presidente RICARDO LORENZETTI y el juez JUAN CARLOS MAQUEDA, por aceptarla parcialmente".

b.5) Panamá

El 18 de julio de 2016 se presentó ante la Asamblea Nacional panameña un anteproyecto de Ley "Que faculta a los usuarios del Internet a exigir a portales y redes sociales que eliminen sus datos personales"[339].

El texto legal contaría con diez artículos, y su objeto sería, según su propia exposición de motivos, que: "la legislación obligará a los Portales de Internet a borrar los datos de la persona, de forma inmediata y completa, si ésta lo reclama de forma explícita y que no existe ninguna razón legítima para retenerlos".

No obstante, el proyecto presentado por el diputado MELITÓN ARROCHA fue finalmente retirado[340] ante las numerosas presiones de la prensa del país, que consideraba este derecho diametralmente opuesto al de libertad de información.

Uno de los aspectos más destacables de este anteproyecto de Ley es que permitía el ejercicio del derecho al olvido por parte de las personas jurídicas, además de las personas físicas[341]. De esta manera se ampliaba el alcance de dicho derecho a la esfera del honor de las personas jurídicas, excediendo su ámbito habitual, limitado a los datos personales.

Asimismo, la ley permitía el ejercicio del Derecho al Olvido ante una multitud de prestadores de servicios de la sociedad de la información, desde los titulares de herramientas de búsqueda hasta proveedores de contenidos online[342]. Aquí reside una diferencia fundamental en relación con la jurisprudencia de otros países latinoamericanos y la STJUE C-131/12. Mientras que éstas han solido optar por la

[339] https://www.prensa.com/politica/Anteproyecto-Ley_LPRFIL20160724_0001.pdf
[340] https://www.prensa.com/sociedad/Arrocha-retirara-anteproyecto-derecho-olvido_0_4538546130.html
[341] Art. 4 del Anteproyecto
[342] Art. 5 del Anteproyecto en relación con el art. 2, en el que se contienen las definiciones.

vía de la desindexación, para lo cual resulta necesario accionar contra los correspondientes buscadores, el legislador panameño planteó la eliminación de los datos personales (o de la persona jurídica) en el origen, siendo incluso posible solicitar a los proveedores de servicios de hosting la eliminación de los datos correspondientes.

6.6.4 Rusia

El presidente Vladimir Putin rubricó el 13 de julio de 2015 la *Ley rusa para la tecnología de la información*[343], en la que se reconoce formalmente en ese país el derecho al olvido. Esa norma, entró en vigor el 1 de enero de 2016[344].

Reconoce el derecho al olvido digital en términos similares al del resto de legislaciones analizadas en este trabajo, con las siguientes excepciones:

- Recoge una excepción expresa a la posibilidad de solicitar la eliminación de información relacionada con los eventos que apuntan a la comisión de hechos con relevancia penal en los que no han expirado los términos correspondientes a la prescripción ni la información sobre la comisión de un delito para el que aún no se haya dictado una condena o ésta aún no se haya cancelado[345].

- La ley solo se aplica a los operadores de motores de búsqueda que se vinculan a sitios web de terceros y no a los sitios web de redes sociales u otros sitios web con motores de búsqueda internos. Además, la ley se aplica solo a los

[343] Zakon ob Informatsii, Informatsionnykh Tekhnologiyakh i o Zaschite Informatsii [Law on Information, Information Technologies] No. 149-FZ, July 27, 2006, SZRF July 31, 2006, No. 31 (Part 1), item 3448, http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, archived at https://perma.cc/B5LU-Q69T.
[344] https://www.hldataprotection.com/2015/12/articles/consumer-privacy/russian-right-to-be-forgotten-law-update/
[345] https://www.loc.gov/law/help/erasure-online-info/russia.php#_ftn7

motores de búsqueda que distribuyen publicidad destinada a atraer la atención de los consumidores ubicados en Rusia.

- Los motores de búsqueda operados por el gobierno y los municipios están excluidos del ámbito de aplicación de la ley.

6.6.5 Japón

El derecho al olvido no se ha reconocido en el ordenamiento positivo japonés, siendo controvertida tanto su aplicación como su alcance, y habiendo optado las autoridades de protección de datos de ese país por promover la autorregulación[346].

Sin embargo, a raíz de la *Sentencia Google*, los casos en los que los particulares han invocado este derecho han ido incrementando, superando en la actualidad los cincuenta. El 31 de enero de 2017, el Tribunal Supremo de Japón dictó por primera vez una Sentencia en la que se abordó la cuestión sobre si debían desindexarse, o no, los resultados ofrecidos por buscadores de Internet, entendiendo ese Alto Tribunal que "el borrado debía permitirse si la protección de la intimidad resulta claramente superior" en el análisis de los derechos en conflicto. Para alcanzar una conclusión sobre qué derecho es prevalente en cada caso hay que atender, según la Corte japonesa, al contenido de la información, la extensión del daño, posición social y otros factores. Como consecuencia de lo anterior, en el caso analizado la petición fue desestimada, ya que el asunto en cuestión aludía a crímenes de pederastia, por lo que el Tribunal Supremo de Japón entendió prevalente, en este caso, las libertades de información y expresión.

[346] FUJIWARA, S.: "Current situation of discussions on Right to be forgotten in Japan"; https://blogdroiteuropeen.files.wordpress.com/2017/06/rtbf-in-japan-6-june-final-version.pdf https://blogdroiteuropeen.files.wordpress.com/2018/04/the-right-to-be-forgotten-in-europe-and-beyond-26-april.pdf

6.6.6. China

La circunstancia del eventual reconocimiento del derecho al olvido digital en la jurisprudencia de la República Popular de China ha causado gran expectación. Al respecto, podemos reproducir, gracias al trabajo del Profesor de la Universidad de Feng Chia en Taichung, HSU PIAO-HAO[347], el contenido de la más reciente jurisprudencia en la materia, y en particular, el de la Sentencia *Baidu*, dictada en 2015[348].

Precisamente en febrero de ese año 2015, el reclamante, Sr. Ren, comenzó a encontrar resultados de búsquedas sobre su persona en el motor de búsqueda Baidu (equivalente chino de Google), gestionado por los denunciados, Baidu Netcom Science and Technology (Beijing) Co., Ltd. Esos resultados implicaban un cierto grado de asociación entre el reclamante y "Tao's Education", una academia situada en la ciudad de Wuxi y de dudosa reputación -entre otras cuestiones, había sido acusada de fraude.

El Sr. Ren trabaja en el ámbito de la gestión de recursos humanos y en el de las operaciones corporativas. Durante el juicio, Mr. Ren presentó un certificado que demostraba que había sido despedido como empleado de la empresa Dao Ya Shuan Commerce & Trade Co., Ltd, como consecuencia de los resultados de las búsquedas efectuadas por los responsables de la compañía en Baidu, y que vinculaban al Sr. Ren con Tao Education, a quienes algunas personas llegaban a considerar una secta.

Sobre la base del derecho al nombre y a la fama y los derechos de la personalidad, el reclamante solicitó a Baidu que eliminase los resultados que vinculaban su nombre con el de Tao´s Education.

---

[347] PIAO HAO HSU: "The Right to Be Forgotten and its ramifications in Taiwan, China and Japan", e-conference on the Right to be Forgotten in Europe and Beyond, June 2017, Blogdroiteuropeen; https://blogdroiteuropeen.com/2017/06/13/the-right-to-be-forgotten-and-its-ramifications-in-taiwan-china-and-japan-by-piao-hao-hsu/

[348] Civil Judgment of People's Court of Haidian District, Beijing, No. (2015) Hai Min Chu 17417

Durante la tramitación del juicio en primera instancia, el Juez determinó que el objeto fundamental del procedimiento era determinar la legalidad, o no, de ese tipo de resultados relacionados y la legitimidad de este servicio. El Juzgado dividió su análisis en dos partes: la primera, relativa al análisis de los hechos y la circunstancia sobre si esos resultados predefinidos eran intervenidos artificialmente, o no, por Baidu. La segunda, centrada en si el modelo técnico de esas búsquedas relacionadas (función de autocompletado) y el servicio prestado por Baidu vulneraba el derecho al nombre, fama y derecho al olvido en la aplicación general de los derechos de la personalidad como argumentaba el reclamante.

Sobre la primera cuestión, el Juzgado entendió que Baidu no intervenía en los resultados de búsqueda por cuanto, de las averiguaciones realizadas por la Corte resultaba que esos resultados variaban en cada ocasión, dependiendo de la frecuencia con que determinadas palabras se buscaban en un determinado periodo temporal -según explicaba Baidu-.

En la segunda parte de su análisis, la Corte concluyó que, en tanto que no hay una intervención "humana" en esos resultados, la queja del Sr. Ren se reducía a analizar si el modelo técnico del servicio de búsquedas relacionadas invadía los intereses del reclamante. En este análisis, el Juzgado estimó que las frases mostradas por el motor de búsqueda objeto de controversia no tenían connotaciones negativas, ni en el fondo ni en la forma. Como consecuencia de lo anterior, el Juzgado determinó que no se habían infringido los derechos del reclamante, por cuanto no se había menoscabado su fama. El Juzgado concluyó de forma tajante que el derecho al olvido no existe en China, resultando improcedente concede la protección solicitada. El Tribunal Superior del Distrito de Haidian concluyó que la aplicación general de los derechos de la personalidad requiere la aplicación de un test de legitimidad entre los intereses en cuestión y la necesidad de protección. La Corte recordó que, en el presente caso, Mr. Ren no era ni menor ni persona necesitada de especial protección cuando cooperó

con Tao's Education, de tal forma que no había justificación legal para la protección impetrada, que debía ser considerada en todo caso excepcional.

La Corte estimó que no existía ni legitimidad en la reclamación ni necesidad de protección legal en el ámbito del "derecho al olvido" que solicitaba el reclamante. Seis meses después, el pronunciamiento de la Corte del Distrito de Haidian fue confirmada en segunda instancia sin alterar sustancialmente sus pronunciamientos.

6.6.7 Australia

En el año 2014, y consecuencia de la *Sentencia Google*, la Comisión para la reforma de las leyes de Australia estudió si debía implantarse un "derecho al olvido digital" en ese país[349], concluyendo que sería interesante la creación de un derecho "al autoborrado" que permitiría eliminar la información publicada por uno mismo[350], pero no la publicada por terceros[351].

[349] https://www.burkemeadlawyers.com.au/commercial-law/right-forgotten-australia/
[350] https://www.alrc.gov.au/publications/15-new-regulatory-mechanisms/new-privacy-principle-deletion-personal-information
[351] http://www.saintylaw.com.au/2014/05/19/eu-right-to-be-forgotten/

CONCLUSIONES

Primera.- El derecho al "olvido digital" es un derecho fundamental de los denominados "de cuarta generación" (a través de los cuáles se quiere dar respuesta a las nuevas necesidades a las que el hombre debe enfrentarse como consecuencia de la revolución tecnológica), y que no constituye sino una extensión del derecho a la autodeterminación informativa, entendido éste como una ramificación del tradicional derecho a la intimidad personal y familiar.

Las primeras formulaciones doctrinales en las que se refleja el concepto de "derecho fundamental a la intimidad" son las de COOLEY y WARREN y BRANDEIS, quienes aludieron por primera vez, de forma respectiva, tanto al "right to be let alone" como al "right to privacy".

El artículo de WARREN y BRANDEIS originó una preocupación colectiva por la protección de la esfera privada del individuo que vive en sociedad, que es respetuosa asimismo de la dimensión social o colectiva, estableciendo también límites sobre ese derecho en beneficio y cuidado del estado democrático.

Revisado y sistematizado posteriormente por WILLIAM L. PROSSER en 1960 y otros estudiosos, esas formulaciones doctrinales fueron conceptualizadas e incluidas de forma paulatina en las Declaraciones de derechos que fueron promulgándose de mediados del Siglo XX en adelante, como así sucedió por primera vez en la *Declaración Americana de Derechos y Deberes del Hombre*, de 2 de mayo de 1948, y posteriormente en las *Declaraciones Universales de Derechos Humanos* de ese mismo año, en el *Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales* de 1950 (art. 8.1) y en el *Pacto internacional de los derechos civiles y políticos* de 1966.

En nuestro ordenamiento nacional, la *Constitución Española de 27 de diciembre de 1978* ampara a través de su art. 18 CE distintos derechos, todos ellos inspirados en el fundamental a la intimidad, pero con perfiles propios: el derecho al honor, a la intimidad personal y familiar y a la propia imagen; la inviolabilidad del domicilio; el secreto de las telecomunicaciones, y el derecho fundamental a la protección de datos.

Ese *derecho a la protección de datos* o *derecho de autodeterminación informativa*, constituye la evolución de una línea jurisprudencial que parte del derecho a la intimidad personal y familiar, pasa por ese derecho a la autodeterminación informativa, y evoluciona hasta la protección de datos de carácter personal, que se reconoce como un "verdadero derecho fundamental autónomo e independiente del derecho a la intimidad", que nuestro TC define como "poder de disposición y control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso".

Segunda.- El germen del derecho al olvido digital en la legislación comunitaria se halla en el reconocimiento que el *Convenio 108 del Consejo de Europa*, de 28 de enero de 1981, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, realiza del "derecho a la calidad de los datos". Ese Convenio es, a día de la fecha, el único instrumento multilateral jurídicamente vinculante en el ámbito de la protección de los datos de carácter personal, y acaba de modernizarse para adaptarse a las novedades legislativas en materia de protección de datos ("Convenio nº 108 +").

Con la entrada en vigor del TCE (12 de junio de 1985) se reconoce en su art. 286 (ahora art. 16.1 TFUE) el derecho de toda persona a la protección de datos personales, encomendando al Parlamento y al Consejo de la UE la aprobación de las normas que

pudieran ser necesarias para la protección de las personas físicas respecto del tratamiento de sus datos de carácter personal.

En ese contexto, el legislador comunitario aprobó en un primer momento la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, que supuso en hito en la regulación de la protección de datos de carácter personal.

Por cuanto respecta a nuestro país, el primer reconocimiento jurisprudencial en España del derecho a la protección de datos de carácter personal como un verdadero derecho independiente y autónomo se produce a través de dos importantísimas Sentencias de nuestro Tribunal Constitucional, dictadas el 30 de noviembre del año 2000 con los números 290 y 292.

La primera norma sustantiva que reconoce específicamente el derecho a la protección de datos personales en España es la Ley Orgánica 5/1992, de 29 de octubre, *de regulación del tratamiento automatizado de los datos de carácter personal* (LORTAD), que supuso un hito en el reconocimiento del derecho a la protección de datos de carácter personal, siendo la primera en cumplir el mandado del apartado 4º del artículo 18 de la CE, y sentando las bases de las normas posteriores, para las que puede considerarse un antecedente fundamental.

La LORTAD fue desarrollada reglamentariamente a través de los Reales Decretos 428/1993, 1332/1994 y 994/1999, por los que se aprobó el Estatuto de la Agencia Española de Protección de Datos; se desarrolló parcialmente la LORTAD y se aprobó el Reglamento de medidas de seguridad, respectivamente.

Todas esas normas fueron derogadas por la posterior entrada en vigor de la Ley Orgánica 15/1999, *de protección de datos de carácter personal*, cuyo objetivo fundamental

fue la trasposición al ordenamiento interno de los postulados de la Directiva 95/46/CE. La LO 15/1999 fue desarrollada reglamentariamente a través del Real Decreto 1720/2007 y complementada por la normativa autonómica de protección de datos (particularmente las leyes catalana, andaluza y vasca).

Tercera.- El TJUE se pronunció por vez primera sobre el alcance y límites del derecho al olvido digital en su Sentencia de 13 de mayo de 2014, dictada en el asunto C-131/12, en el procedimiento entre Google España S.L., Google Inc. vs. AEPD y Mario Costeja González (*Google vs. España*), que es uno de los asuntos con mayor transcendencia social y repercusión jurídica de los últimos años.

El supuesto de hecho que se analiza en la misma es el siguiente: en el año 1998, el periódico "La Vanguardia" publicó dos anuncios relativos a una subasta de inmuebles en los que se citaba al embargado con nombre y apellidos. Esa subasta estaba relacionada con deudas de la Seguridad Social. Con posterioridad a esa fecha, el medio digitalizó su hemeroteca, y esa noticia se puso a disposición del público a través de Internet.

En el mes de noviembre de 2009, el Sr. Costeja contactó con el periódico ejercitando su derecho de oposición al tratamiento de sus datos de carácter personal, al considerar que aquella deuda era una asunto arreglado y zanjado hacía muchos años y que en el año 2009 carecía de interés.

El medio desatendió la reclamación del Sr. Costeja, quien la reprodujo ante Google España, quien respondió reenviando al Sr. Costeja ante Google Inc., aludiendo que esa empresa americana es quien presta el servicio de buscadores.

Mario Costeja se dirigió entonces a la Agencia Española de Protección de Datos, formulando una reclamación ante La Vanguardia, Google España y Google Inc. que

fue estimada mediante resolución de fecha 30 de julio de 2010 (R/01515/2010, de 30 de julio de 2010). En esa resolución, la Agencia Española de Protección de Datos estimó la reclamación frente a Google España y Google Inc. Pero la rechazó contra La Vanguardia, al entender que la publicación en dicho medio tendría justificación legal. Tanto Google España como Google Inc. recurrieron esa resolución ante la Sala de lo contencioso-administrativo de la Audiencia Nacional.

Mediante Auto de fecha 27 de febrero de 2012, núm. 19/2012, la Audiencia Nacional acotó el objeto de controversia a "determinar las obligaciones que tienen los gestores de los motores de búsqueda en la protección de datos personales de aquellos interesados que no desean que determinada información publicada en páginas web de terceros, que contienen sus datos personales y permite relacionarles con la misma, sea localizada, indexada y puesta a disposición de los internautas de forma indefinida".

Al considerar que la interpretación de esta cuestión dependía de la que se hiciera de la Directiva 95/46 de Protección de Datos de las Personas Físicas, la Sección 1ª de la Sala de lo contencioso-administrativo de la Audiencia Nacional que estaba conociendo del asunto acordó formular nueve cuestiones prejudiciales de interpretación ante la Corte de Justicia de la Unión Europea, y que se recogen en el citado Auto de 27 de febrero de 2012.

El TJUE aborda y resuelve positivamente todas ellas en su Sentencia de 13 de mayo de 2014.

Cuarta.- La Sección 1ª de la Sala de lo contencioso-administrativo de la Audiencia Nacional, acogió los argumentos del TJUE al resolver el recurso contencioso interpuesto por Google España en Sentencia de 29 de diciembre de 2014 (recurso 725/2010), acordando desestimar el recurso contencioso administrativo interpuesto

por Google, y confirmar la adecuación a Derecho de la Resolución dictada por el Director de la Agencia Española de Protección de Datos al inicio de la controversia. La entidad Google España, S.L. interpuso frente a esa Sentencia de la Audiencia Nacional recurso de casación en el que se hacen valer cuatro motivos de casación, el primero articulado a través del artículo 88.1.c) de la LJCA (RCL 1998, 1741) y los otros tres con base en la letra d) de este mismo precepto.

El Tribunal Supremo estimó ese recurso mediante Sentencia de la Sección 6ª de la Sala de lo contencioso-administrativo del Tribunal Supremo, núm. 1611/2016 de 4 julio, al entender que debió estimarse el recurso contencioso-administrativo de Google España, manteniendo todos los pronunciamientos frente a Google Inc.

El Tribunal Supremo acoge los argumentos de Google España en el exclusivo sentido de estimar su falta de legitimación pasiva y reenvía a los afectados por el tratamiento de sus datos personales a ejercitar sus derechos ante la matriz, Google Inc., con sede en California. Y ello en el entendimiento de que Google España no es responsable de ese tratamiento en los términos en que ese concepto es entendido por el nuevo Reglamento Europeo de Protección de Datos, ni puede concluirse tal cosa de otras actuaciones anteriores de la aludida compañía, ni tal conclusión no puede extraerse tampoco del mero hecho de ser ambos una unidad de negocio. No obstante lo anterior, mantiene el resto de pronunciamientos de la Sentencia de instancia en relación con el reconocimiento del derecho al olvido.

Sin embargo, y en contraste con lo anterior, la Sala de lo civil del Tribunal Supremo (es ejemplo la Sentencia núm. 210/2016 de 5 abril, del Pleno de la Sala de lo Civil del Tribunal Supremo) si ha atribuido responsabilidad a Google España en asuntos de tutela de protección de datos. En particular, cree esa Sala del TS que sí es posible dirigirse en vía civil frente a Google España en procedimientos de tutela de derechos, ya que otra cosa haría prácticamente imposible su ejercicio, abocando a los interesados a procesos judiciales largos y costosos. En el criterio de la Sala de lo civil es posible

ejercitar esos derechos frente a Google España ya que tiene consideración de "responsable" en nuestro país del tratamiento efectuado por Google en el sentido establecido por la Sentencia del TJUE de 2014.

No deja de ser chocante que dos Salas de un mismo Tribunal alcancen soluciones dispares respecto de un mismo problema, circunstancia que refleja que el derecho al olvido digital es un derecho en construcción, que plantea esas y otras muchas dudas prácticas para su aplicación (¿qué sucedería si, en vez de nombre y apellidos, se inserta en el buscador un pseudónimos, diminutivos o nombres familiares que permitieran de la misma manera la identificación del afectado? ¿qué hacer en el escenario inverso?, esto es, si en el buscador se introduce o bien una palabra malsonante o insulto, o bien una conducta delictiva o reprobable, y que el nombre de una persona con nombre y apellidos apareciera en la lista de resultados arrojados por el buscador. ¿Y si son dos personas con los mismos nombres y apellidos?).

Pueden suscitarse, también, problemas de prestación del consentimiento en redes sociales por padres respecto de sus hijos menores, o dudas respecto de la aplicación territorial de los derechos objeto de análisis.

Quinta.- En los cinco años que han transcurrido desde el dictado de la *Sentencia Google* el 29 de mayo de 2014 y hasta el mes de agosto de 2019, el gigante de Internet Google ha recibido, a través de una herramienta específicamente implementada al efecto, más de 800.000 solicitudes de desindexación (834.733), que afectaban a 3.281.701 URL, de las que ha suprimido 1.199.955 –el 44,5% de las peticiones–. De todas estas, el 88,6% las habían promovido personas particulares; el resto correspondían a menores de edad, entidades corporativas, políticos y personas con cargo o relevancia pública. De esas más de 800.000 solicitudes, 79.710 se realizaron desde España, e incumbían a 261.125 URL. De esas solicitudes, el buscador ha suprimido 81.813 enlaces, el 37,9%.

En la evaluación de esas solicitudes, Google debe realizar un balance entre los derechos del usuario y el interés público que, en su caso, pudiera suscitar el contenido. El sitio web más afectado por esas solicitudes es Facebook, con 47.418 urls.

Por su parte, la AEPD recibió en el año 2.018 mil setecientas ochenta y cuatro reclamaciones sobre el ejercicio de todos los derechos de protección de datos -acceso, rectificación o cancelación-. De ellas, casi 200 (191) corresponden a reclamaciones por derecho al olvido. La proporción estimadas/desestimadas de estas 191 tutelas/reclamaciones es prácticamente de un 50%. En cuanto a las entidades reclamadas, Google y sus servicios aglutinan 125 de las 191 (65%), 18 a medios de comunicación (9%), 14 a otros buscadores de Internet (7%), 13 corresponden a Administraciones Públicas y boletines (6%), cifras que se completan con un apartado de peticiones a Otras entidades.

Sexta.- Es en el art. 17 del RGPD en el que el derecho al olvido se consagra de forma definitiva como un nuevo derecho, aunque no deja de ser, como ha indicado la doctrina mayoritaria, un derecho nuevo manifestación de otros derechos y principios ya existentes, como el derecho de cancelación y el principio de calidad de los datos, tratándose "de la propia evolución de los derechos de cancelación y oposición, al compás del avance de las nuevas tecnologías y del avance de Internet".

Esa norma se aplica de forma directa en todos los Estados miembros de la UE desde el 25 de mayo de 2018. Sin perjuicio de esa aplicación directa, algunos Estados miembros han aprobado -o están aprobando- normas para la adaptación de su normativa interna al contenido del RGPD UE (son ejemplos: Alemania, Italia, Francia, Reino Unido, España y Portugal).

La entrada en vigor en España el 25 de mayo de 2018 pasado del RGPD de la UE, supuso el desplazamiento de todas las disposiciones de Derecho interno que no se acomodasen a lo dispuesto en el aludido reglamento comunitario. Esta circunstancia tuvo, durante un determinado periodo temporal, impacto sobre muchos preceptos tanto de la LOPD como de su reglamento de desarrollo (RD 1720/2007).

Con vocación de adaptar de forma inmediata la normativa de protección de datos nacional al RGPD se aprueba, a finales del mes de julio del año 2018, el "Real Decreto-ley de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos". A través de dicho texto se adaptaron por el legislador nacional al Reglamento europeo, de forma inmediata, aquellos aspectos de la normativa de protección de datos que no son objeto de reserva de Ley Orgánica, y en tanto se procedía a la completa revisión del marco normativo mediante la aprobación de esa preceptiva nueva LO (Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales*), publicada en diciembre de 2018, y en la que se produce el reconocimiento positivo del derecho al olvido digital en la legislación española (arts. 93 y 94 del texto de LO).

Desde la aprobación definitiva de ese texto, y su publicación y entrada en vigor en diciembre de 2018, España es uno de los primeros países que ha reconocido de forma positiva y expresa en su normativa interna el "derecho al olvido digital", tanto desde la perspectiva del derecho a no ser indexado por los motores de búsqueda cuando la información que esa búsqueda arroje sea inexacta, inadecuada o impertinente, o hubiera adquirido esa condición por el paso del tiempo; como desde la perspectiva del derecho a que los datos de una persona sean suprimidos de los servicios de redes sociales (u otros equivalentes de la sociedad de la información), a su sola solicitud.

Séptima.- El día 15 de octubre de 2015, el Pleno de la Sala primera del Tribunal Supremo dictó en el recurso de casación núm. 2772/2013, la primera Sentencia de ese Alto Tribunal en la que se aborda el tratamiento que debe darse al denominado "derecho al olvido digital" en caso de conflicto con el derecho a la libertad de información, entendido hasta el momento como la facultad de una persona de solicitar de un motor de búsqueda en Internet, la desindexación de entre los resultados que arroja la búsqueda por su nombre y apellidos de aquellas informaciones que, a pesar de haber sido exactas históricamente, han devenido imprecisas por el paso del tiempo, y cuya divulgación a día de la fecha afecta negativamente a su reputación.

La Sala, con cita a las Sentencias del TJCE dictadas en los asuntos Lindqvist (C-101/01, apartado 25) y Google (C-131/12, párrafo 26), estima que el editor de una página web en la que se incluyen datos personales realiza un tratamiento de datos, y por tanto es responsable de que ese tratamiento cumpla las exigencias de la normativa que lo regula, y en particular las derivadas del principio de calidad de los datos (adecuación, pertinencia, exactitud y proporcionalidad). Por tal motivo, extiende las conclusiones alcanzadas por el Tribunal de Justicia de la Unión Europea en el asunto Google sobre las obligaciones de los gestores de motores de búsqueda a los editores de páginas web, considerando que los mismos son también responsables del tratamiento de datos, al serles técnicamente factible atender las solicitudes de desindexación mediante la introducción de comandos de exclusión (robot.txt o códigos "noindex" "noarchive"), obligaciones que se derivan tanto de la propia Constitución como del Convenio Europeo de Derechos Humanos, de la Carta de derechos fundamentales de la Unión Europea, del Convenio núm. 108 del Consejo de Europa de 28 de enero de 1981, así como de la Directiva de protección de datos, la LO 15/1999, y la jurisprudencia que ha interpretado todas esas normas.

En el criterio de la Sala, los principios de adecuación, pertinencia, proporcionalidad y exactitud que conforman la calidad de los datos (art. 6 de la Directiva y 4 de la LOPD) deben analizarse considerando muy especialmente el "factor tiempo" ya que un

tratamiento que "inicialmente pudo ser adecuado a la finalidad que lo justificaba" puede "devenir con el transcurso del tiempo inadecuado para esa finalidad", causando un daño desproporcionado en los derechos de la personalidad al honor y la intimidad.

El derecho a la protección de datos del art. 18 CE se invoca en el supuesto analizado de forma indisolublemente vinculada a otros derechos consagrados en ese mismo art. 18 (honor e intimidad personal y familiar, a los que está íntimamente ligado), siendo desde esa perspectiva del análisis del alcance y límites de ese derecho fundamental que se pronuncia por primera vez la Sala civil del TS y sobre las que hasta ese momento solo había tenido ocasión de pronunciarse la Sala de lo contencioso-administrativo, en aplicación de la función revisora de esa Sala respecto de las valoraciones realizadas por la AEPD.

Al igual que ocurrió al dictarse aquella Sentencia por el TJCE, sucede en el presente caso que el Tribunal deja claro que la ponderación ha de hacerse caso por caso, como se viene haciendo desde siempre en los conflictos entre los derechos del art. 18 CE con los del art. 20 CE, y sin poder instaurar de forma apriorística criterios universales que puedan aplicarse de forma general a todos los supuestos, aunque si sea posible sentar algún tipo de directriz o guía como las que el Grupo de trabajo del art. 29 ha procurado establecer para la aplicación de la *Sentencia Google*, y que de forma velada han sido tenidas en consideración por al el TS en su pronunciamiento.

No obstante, existen dos diferencias importantes que deben destacarse entre el supuesto sometido al criterio del TS y el que le ha servido de antecedente y que son, en primer término, como ese Tribunal Supremo emplea en la redacción de la Sentencia objeto de análisis especial celo en imposibilitar la identificación de las dos personas demandantes, omitiendo deliberadamente datos y fechas que pudieran permitir su reconocimiento, precisamente para respetar la finalidad buscada con el impulso de ese procedimiento judicial, que era proteger su privacidad y su anonimato.

No solo el Tribunal evita en todo momento mencionar a los recurrentes tanto en el encabezamiento de la Sentencia (aludiéndoles genéricamente como "A" y "B") como en el cuerpo y fallo de la misma, sino que se refiere a los mismos como "las dos personas demandantes", evitando en todo momento su identificación. Decisión que resulta especialmente llamativa si se compara con el pronunciamiento judicial que le ha servido de "antecedente" y que no es otro que la Sentencia del TJCE en el caso Google, en la que el reclamante de olvido, Sr. Costeja, será indefinidamente recordado precisamente por querer ser olvidado. Ironías de la vida.

La segunda diferencia que debe reseñarse es que la Sentencia del TS extiende la responsabilidad del encargado de la gestión de los motores de búsqueda a los editores de páginas web en la que se emplean datos personales, incidiendo especialmente en la posibilidad técnica que esos responsables tienen de desindexar las páginas objeto de controversia mediante la inclusión en sus cabeceras de los comandos informáticos adecuados.

La Sala modula acertadamente en esa resolución la responsabilidad de los responsables de los buscadores, entendiendo que esa responsabilidad no sería objetiva ni derivada de la mera digitalización del contenido, sino que exige se haya producido por el afectado un requerimiento previo al medio, disponiendo expresamente que "no puede exigirse al editor de la página web que por su propia iniciativa depure estos datos" porque ello supondría "un sacrificio desproporcionado para la libertad de información" a la vista de "las múltiples variables que debería tomar en consideración y de la ingente cantidad de información objeto de procesamiento y tratamiento en las hemerotecas digitales". Y que lo que "si puede exigírsele" es que "dé una respuesta adecuada a los afectados que ejerciten sus derechos de cancelación y oposición al tratamiento de datos y que cancele el tratamiento de sus datos personales cuando haya transcurrido un período de tiempo que haga inadecuado el tratamiento, por carecer las personas afectadas de relevancia pública, y no tener interés histórico la vinculación de la información a sus datos personales".

Por ello, en este caso la condena del Tribunal Supremo viene motivada específicamente por "la denegación por Ediciones El País de la cancelación del tratamiento de sus datos personales ante la solicitud hecha por las personas demandantes" que se entiende supuso "una vulneración del derecho de protección de datos personales de las personas demandantes que trajo consigo la intromisión ilegítima en sus derechos al honor y a la intimidad".

Las conclusiones alcanzadas por el Tribunal Supremo no parecen desacertadas ni alejadas de las previamente establecidas por el TJCE en la *Sentencia Google*, si bien se plantea, como sucedió al dictarse aquella sentencia, el interrogante de cómo se aplicará esa jurisprudencia a cada uno de los supuestos diferenciados que puedan darse en el futuro, pudiendo establecerse de antemano unas directrices generales o guías de aplicación, pero debiendo realizarse dicho análisis, como se ha venido haciendo hasta la fecha en los supuestos en los que se produce una colisión entre los derechos del art. 18 con los del 20 CE, caso por caso.

Octava.- Frente a la aludida Sentencia del Tribunal Supremo, se interpuso por los reclamantes recurso de amparo, seguido con el núm. 2096-2016 ante la Sala Primera del Tribunal Constitucional y resuelto mediante Sentencia de 4 de junio de 2018.

En la misma, el Tribunal Constitucional configura, por vez primera, el "derecho al olvido digital" en nuestra jurisprudencia constitucional, de la siguiente forma: "el derecho a obtener, sin dilación indebida, del responsable del tratamiento de los datos personales relativos a una persona, la supresión de esos datos, cuando ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados; cuando se retire el consentimiento en que se basó el tratamiento; cuando la persona interesada se oponga al tratamiento; cuando los datos se hayan tratado de forma ilícita; cuando se daba dar cumplimiento a una obligación legal establecida en el Derecho de la Unión

o de los Estados miembros; o cuando los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de información".

En la Sentencia analizada, ese Alto Tribunal, define por primera vez en la jurisprudencia constitucional el derecho al olvido como "una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4 CE)", y como "mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo".

Novena.- Por su parte, el Tribunal Europeo de Derechos Humanos también se ha sumado a la "corriente" de la *Sentencia Google* y ha dictado su primera Sentencia en la que se alude de forma expresa a ese "derecho al olvido digital".

Se trata de la Sentencia del TEDH de 28 de junio de 2018, M.L y W.W c/ Alemania, en la que ese Tribunal Europeo de Derechos Humanos (TEDH) se ha pronunciado por primera vez en un asunto en el que por los reclamantes se invocaba la vulneración del art. 8 del CEDH por motivo de la negativa de anonimización de determinadas informaciones incluidas en hemerotecas digitales, que les incumbían.

No obstante, considerando las particulares circunstancias del supuesto sometido a enjuiciamiento, en este caso el TEDH determina que, en su criterio, Alemania no ha vulnerado ese derecho, y ello considerando: (i) El margen de apreciación de las autoridades nacionales respecto del balance a efectuar entre los derechos en juego; (ii) La importancia de mantener disponibles publicaciones cuya legalidad no fue puesta en cuestión en el momento de su publicación y, (iii) la propia conducta de los reclamantes en relación con la prensa.

Por esas tres razones, la Corte no ve motivos sólidos por los que deba sustituir el criterio de los Tribunales alemanes por el suyo propio, considerando que Alemania no habría vulnerado el art. 8 de la CEDH al primar, en el primer caso sujeto al criterio de ese Tribunal, el derecho a las libertades informativas frente al invocado derecho al olvido digital.

Además, puntualiza el TEDH que las obligaciones de los motores de búsqueda respecto de las personas concernidas "podrían ser distintas de las de los medios de comunicación al origen de esas informaciones", pudiendo ser diferente el balance de los intereses en conflicto dependiendo de si los mismos involucran a quienes están "al origen y corazón de la libertad de expresión" o aquéllos cuyo objetivo no es publicar "sino facilitar su identificación y la localización de la información", pero subrayando asimismo que esos motores de búsqueda no habrían sido llamados al procedimiento ni se habría presentado ningún tipo de reclamación frente a los mismos.

Décima.- La aplicación directa de lo dispuesto en el art. 17 del Reglamento General de protección de datos, determina que el derecho al olvido digital esté reconocido en todos los países integrantes de la Unión Europea. Si bien, ese derecho se ha implementado con matices en unos y otros Estados, destacando los desarrollos jurisprudenciales que han tenido lugar en Reino Unido, Italia, Alemania, Suecia, Bélgica o Francia a los que aludimos en el Capítulo 6 del presente trabajo.

De todos ellos, el más relevante es ese último (el francés), y ello considerando que el 19 de julio de 2017, el Consejo de Estado francés elevó a la Corte de Justicia de la Unión Europea una nueva cuestión prejudicial concerniente al derecho de desindexación o al derecho al olvido digital, y en particular, sobre la forma en la que, según la Corte de Justicia de la Unión Europea, debería interpretarse el alcance territorial de ese derecho.

El asunto, resuelto mediante Sentencia de 24 de septiembre de 2019 (asunto C-507717), el TJUE ha acogido los argumentos sostenidos por la mercantil Google, según quienes las pretensiones del Francia y la CNIL de aplicación universal de la obligación de desindexación no podían acogerse, ya que ni los estándares de los derechos a la libre información/expresión ni los de la protección de datos son los mismos en todo el mundo ni los pronunciamientos de esa Sentencia pueden aplicarse más allá del ámbito de aplicación de la norma. Interpretación que también fue sostenida por el Abogado General en sus conclusiones, publicadas el 10 de enero de 2019.

Además de en Francia, los postulados del TJUE en la *Sentencia Google* han tenido impacto, sea a través de desarrollos normativos, sea a través de pronunciamientos jurisprudenciales, más allá de los ordenamientos de los países integrantes de la Unión Europea. Sería el caso de países como Costa Rica, Nicaragua y Uruguay, que han reconocido -positivamente el derecho al olvido digital en sus ordenamientos.

También han reconocido ese derecho, por medio de la jurisprudencia, Chile, Perú, Argentina, Panamá o Colombia, que es un referente mundial en el reconocimiento del derecho al olvido digital, por cuanto la Sentencia de la Corte Constitucional Colombiana T-414/92 reconoció por primera vez este derecho en una resolución dictada veintidós años antes de la Sentencia del TJUE.

Resulta interesante verificar como el problema abordado por el TJUE se reproduce de forma muy similar en otros países ajenos al ordenamiento comunitario, como puedan serlo los citados, y como en la mayoría de los supuestos se están adoptando soluciones parecidas a la que es objeto de estudio en el presente trabajo (son ejemplos Rusia o Australia).

BIBLIOGRAFÍA

---

1. LIBROS:

- **ALONSO, L. y VÁZQUEZ, V.J.:** *Sobre la libertad de expresión y el discurso del odio*, 1ª Edición, Athenaica Ediciones Universitarias, Sevilla, 2017.

- **ALDERMAN, E. y KENNEDY, C.:** *The right to privacy*. Ramdom House Inc., New York, 1995.

- **ÁLVAREZ CARO, M.:** *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. 1º Edición, Ed. Reus, Madrid 2015.

- **APARICIO VAQUERO, J.P. y BATUECAS CALETRÍO, A. (Coordinadores):** *En torno a la privacidad y la protección de datos en la sociedad de la Información*, Ed. Comares, Granada 2013.

- **BARRIO ANDRÉS, M.:** *Fundamentos del derecho de Internet*. Ed. Centro de Estudios Políticos y Constitucionales, Madrid 2017.

- **BARRIO ANDRÉS, M.:** *Internet de las cosas*. Ed. Reus, Madrid 2018.

- **BARRIO ANDRÉS, M.:** *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de Internet*. Ed. Tirant lo Blanch, Valencia 2018.

- **BERROCAL LANZAROT, A.:** *Derecho de supresión de datos o derecho al olvido*. Colección jurídica general. Monografías. Ed. Reus, S.A. Madrid, 2017.

- **BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador):** *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

- **COOLEY, T.:** *A Treatise on the Law of Torts or the Wrongs which arise independent of contract*, Callaghan 2º Ed. Chicago 1888.

- **DAVARA RODRIGUEZ, M.A.:** *Manual de Derecho informático*, Ed. Aranzadi, 11º Edición, Pamplona 2015.

- **DIEZ-PICAZO, L.M.:** *Sistema de Derechos Fundamentales*, Ed. Civitas, 4ª Edición, Madrid 2013.

- **GARCÍA ROCA, J. y SANTOLAYA, P. (Coordinadores):** *La Europa de los derechos. El convenio Europeo de Derechos Humanos*, Ed. Centro de Estudios Políticos y Constitucionales, 2ª Edición, Madrid, 2009.

- **GARRIGA DOMÍNGUEZ, A.:** *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la Computación Ubicua.* Ed. Dykinson, S.L. Madrid, 2015.

- **GRIMALT SERVERA, P.:** *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, Ed. Iustel, Madrid 2007.

- **GUICHOT, E.** (Coordinador): *Derecho de la comunicación*, Ed. Iustel, 5ª Edición, Madrid, 2018.

- **HERNÁNDEZ LÓPEZ, J.M.:** *El Derecho a la Protección de Datos personales en la Doctrina del Tribunal Constitucional*, Ed. Thomson Reuters Aranzadi, Pamplona 2013.

- **HUBMANN, H:** *Das Persönlichkeitsrecht*, Auflage, Köln/Graz, Böhlau, 1967 (1ª edición, 1953), ps. 267 y ss.

- **IBAÑEZ JIMÉNEZ, J. W.:** *Blockchain: Primeras cuestiones en el ordenamiento español.* Ed. Dykinson, S.L. Madrid, 2018

- **MADRID CONESA, F.:** *Derecho a la intimidad, informática y Estado de Derecho*, Universidad de Valencia, Valencia, 1984

- **MARTÍN-RETORTILLO, L.:** "Los derechos fundamentales y la constitución", Ed. El Justicia de Aragón, Zaragoza 2009.

- **MUÑOZ MACHADO, S.:** L*ibertad de prensa y procesos por difamación*, Ed. Ariel, Barcelona, 1988.

- **MUÑOZ MACHADO, S.:** *La regulación de la Red. Poder y Derecho en Internet*, Ed. Taurus, 2000.

- **MUÑOZ MACHADO, S.:** *Tratado de derecho administrativo y derecho público general*, Ed. Iustel, Madrid 2011.

- **MUÑOZ MACHADO, S.:** *Los itinerarios de la libertad de palabra*, Ed. Crítica, Barcelona 2013.

- **MUÑOZ MACHADO, S.** (director): *Diccionario del Español Jurídico* elaborada por la Real Academia de la Lengua Española junto con el Consejo General del Poder Judicial. Espasa. Madrid, 2016.

- **MUÑOZ-MACHADO, S (Ed.).:** *Comentario mínimo a la Constitución Española*, Ed. Crítica, Madrid, 2018.

- **MURILLO DE LA CUEVA, P.L. y PIÑAR MAÑAS, J.L.:** *El derecho a la autodeterminación informativa*. Fundación coloquio jurídico europeo, Madrid 2009.

- **PECES-BARBA MARTÍNEZ, G.:** *Derecho positivo de los derechos humanos*, Madrid, Ed. Debate, 1985.

- **PIÑAR MAÑAS, J.L. (Director) y ALVAREZ CARO, M./RECIO GAYO, M. (Coordinadores):** *Reglamento General de protección de datos. Hacia un nuevo modelo europeo de privacidad.* Ed. Reus, Madrid 2016.

- **PIÑAR MAÑAS, J.L. (Director):** *Smart cities. Derecho y técnica para una ciudad más habitable.* Ed. Reus, Madrid, 2017.

- **RALLO, A.:** *El derecho al olvido en Internet. Google vs. España*. Colección "cuadernos y debates", Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

- **ROBERTSON, A.H.:** *Privacy and human rights*, Ed. Manchester University Press, London 1973.

- **RODRIGUEZ PIÑEIRO Y BRAVO FERRER, M y CASAS BAAMONDE, M.E.:** *Comentarios a la Constitución Española; XL Aniversario*, Ed. Fundación Wolters Kluwer, Boletín Oficial del Estado, Tribunal Constitucional y Ministerio de Justicia Madrid, 2018.

- **RUIZ MIGUEL, C.:** *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Cuadernos Cívitas, Ed. Cívitas, Madrid, 1994.

- **SIBILA, P.:** *La intimidad como espectáculo*. Ed. Fondo de cultura económica de Argentina, S.A., Buenos Aires, 2008.

- **SIMÓN CASTELLANO, P.:** *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia TJUE de mayo de 2014*. 1ª Edición. Ed. Bosch, Barcelona 2015.

- **SIMÓN CASTELLANO, P.:** *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, 2012.

- **TOURIÑO, A.:** *El derecho al olvido y a la intimidad en Internet*, Ed. Catarata, Madrid, 2014.

- **WESTIN, A.:** *Privacy and freedom*, Ed. Atheneum, New York, 1967.

2. ARTÍCULOS:

- **ARCE JARANIZ, A.:** "El derecho de la intimidad. De Samuel D. Warren y Louis D. Brandeis", *Revista Española de Derecho Constitucional*, Año 16. Núm. 47. Mayo-Agosto 1996.

- **BENITO MARTÍN, R.:** "La evaluación del impacto en protección de datos tras el RGPD". *Certamen de artículos jurídicos sobre Derecho del entretenimiento 2016* Premios DENAE, Ed. DENAE, Madrid 2016.

- **BOIX PALOP, A.:** "El equilibrio entre los derechos del artículo 18 de la Constitución, el "Derecho al olvido", y las libertades informáticas tras la Sentencia Google", *Revista General de Derecho Administrativo* nº 38. Ed. Iustel (2015).

- **BUISÁN GARCÍA, N.:** "El derecho al olvido: el nuevo contenido de un derecho antiguo". *El Cronista del Estado Social y democrático de derecho núm. 46*, págs. 22 a 35. Ed. Iustel. Madrid, junio 2014.

- **CASINO RUBIO, M.:** "El periódico de ayer, el derecho al olvido en Internet y otras noticias". *Revista Española de Derecho Administrativo núm. 156*, Octubre-Diciembre de 2012, págs. 201 a 213.

- **CASTÁN TOBEÑAS, J.: "**Los derechos de la personalidad", *Revista General de Legislación y Jurisprudencia*, julio-agosto 1952, págs. 5-62.

- **CAVANILLAS MÚGICA, S. y GRIMALT SERVERA, P.:** "Honor, intimidad y propia imagen", *Base de conocimiento jurídico*, Ed. IUSTEL.

- **DADER, J.S.:** "La privacidad como excusa para restringir la información de interés público", *Revista General de Derecho constitucional, núm. 15,* Ed. IUSTEL, Madrid 2012.

- **DEL NINNO, A.:** "Il "diritto all'oblio" su Internet in Italia: prescrizioni del Garante per la privacy". http://www.dirittoegiustizia.it/news/17/0000068206/Il_diritto_all_oblio_su_Internet_in_Italia_prescrizioni_del_Garante_per_la_privacy.html?cnt=27

- **DEZIEL, P-L.:** "Le Droit a l'oubli au Canada: L'affaire Globe 24h et le role du juge dans les requetes de dereferencement". https://blogdroiteuropeen.com/2017/06/01/le-droit-a-loubli-au-canada-laffaire-globe24h-et-le-role-du-juge-dans-les-requetes-de-dereferencement-pierre-luc-deziel/

- **FUERTES, M.:** "Internet: La paz del camino". *El Cronista del Estado social y democrático de derecho, núm. 37*. Madrid, mayo 2013.

- **FUJIWARA S.:** "Current situation of discussions on Right to be forgotten in Japan"; https://blogdroiteuropeen.files.wordpress.com/2017/06/rtbf-in-japan-6-june-final-version.pdf https://blogdroiteuropeen.files.wordpress.com/2018/04/the-right-to-be-forgotten-in-europe-and-beyond-26-april.pdf

- **GARROTE FERNÁNDEZ-DÍEZ, I.,** "Indemnización por daños morales derivados de la publicación de resultados de buscadores que afectan al derecho al honor e intimidad y a la protección de datos personales", *Revista de Propiedad Intelectual*, núm. 54, 2016, págs. 13-66.

- **GONZALEZ CARILLO, A.:** "Regulación de las noticias falsas (fake news): desafíos y avances en la Unión Europea". *Centro de Estudios internacionales Gilberto Bosques. Análisis e investigación*. 12.2.2018.

- **GÓMEZ-JUAREZ SIDERA, I.:** "Desafíos jurídicos de la nueva robótica para la protección de datos y la privacidad", *Certamen de artículos jurídicos sobre Derecho del entretenimiento 2016* Premios DENAE, Ed. DENAE, Madrid 2016.

- **GUICHOT, E.:** "La publicidad de datos personales en Internet por parte de las Administraciones públicas y el derecho al olvido", *Revista Española de Derecho Administrativo, núm. 154*, año 2012, págs. 125-169.

- **GUICHOT, E.:** "El reconocimiento y desarrollo del derecho al olvido en el derecho europeo y español", *Revista de Administración Pública*, 209, 45-92.

- **HENKEL:** "Der Strafschutz des Privatlebens gegen indiskretion" en *Verhandlugen des Zweiundvierzigsteb Deutschen Juristentages*, Dusseldorf,1957, Tubingen, C,B.Mohr, 1959, p. 60 y ss

- **HERNÁNDEZ RAMOS, M.:** "Motores de búsqueda y derechos fundamentales en Internet. La STJUE Google C-131-12, de 13 de mayo de 2014". *Revista General de Derecho Europeo núm. 31*. Ed. IUSTEL. Madrid 2014.

- **JONASON, P.:** "The digital right to be forgotten in Sweden: the theory and practice of privacy protection mechanisms in the face of referencing by search engines". Droit a ´'oubli en Europe et au-delà.

- **LAZER, D., BAUM, M., BENKLER, Y. y OTROS:** "The Science of fake news: addressing fake news requires a multidisciplinary effort". *Science Magazine*. 9 marzo 2018, volume 359, Issue 6380. Siencemag.org.

- **LEUCCI, S.:** "Diritto all'oblio, verità, design tecnológico: una prospettiva di ricerca. *Media Law*.

- **LÓPEZ, E.:** "Derecho al olvido en la red"; 8.8.2011, Diario La Razón.

- **MAROTO CALATAYUD, M. y otros:** "Reseña de jurisprudencia del Tribunal Europeo de Derechos Humanos (Octubre 2004 - Abril 2005)"; TEDH (Octubre 2004 - Abril 2005), *Revista General de Derecho Europeo*, n.º 3, Ed. Iustel, mayo 2005.

- **MARTINEZ LÓPEZ-SÁEZ, M.:** "Los nuevos límites al derecho al olivo en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de datos personales". *Estudios de Deusto: revista de la Universidad de Deusto*, ISSN 0423-4847, Vol. 65, Nº. 2, 2017, págs. 139-176.

- **MINERO ALEJANDRE, G.:** "A vueltas con el derecho al olvido. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", RJUAM, nº 30, 2014-II. Pp. 129-155.

- **MORACHIMO, M.:** "El discreto desembarco del Derecho al Olvido en Perú", https://revistaideele.com/ideele/content/el-discreto-desembarco-del-derecho-al-olvido-en-per%C3%BA

- **MORENO NAVARRETE, M.A.:** "Aspectos jurídicos privados de las tecnologías web 2.0 y su repercusión en el derecho a la intimidad", en **BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador):** *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

- **MORILLAS FERNÁNDEZ, M.:** "La protección jurídica del menor ante las redes sociales", en **BOIX REIG, J. (Director), JAREÑO LEAL, A. (Coordinador):** *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

- **MORTSIEFER, M.:** "The german battle with fake news", Readings, Eastern Europe and beyond, http://www.eesc.lt/uploads/news/id1059/Readings%202018%201.pdf

- **MUÑOZ MACHADO, S.:** "Internet y los derechos fundamentales" *Anales de la Academia de ciencias morales y políticas" núm. 90*, págs. 491 a 501.

- **MUÑOZ MACHADO, S.:** "Los tres niveles de garantías de los derechos fundamentales en la Unión Europea: problemas de articulación"; *Revista de Derecho Comunitario Europeo*; ISSN 1138-4026, núm. 50, Madrid, enero/abril (2015), págs. 195-230

- **MURILLO DE LA CUEVA, P.L.:** "La construcción del derecho a la autodeterminación informativa". *Revista de estudios políticos, núm. 104*. Abril-junio 1999.

- **MURILLO DE LA CUEVA, P. L.:** "La distancia y el olvido. A propósito del derecho a la autodeterminación informativa", *Revista de jurisprudencia El Derecho*, octubre de 2012.

- **MURILLO DE LA CUEVA, P. L.:** "Informática y Protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del

Tratamiento Automatizado de los Datos de Carácter Personal)". *Cuadernos y Debates nº 43*. Centro de Estudios Constitucionales. Madrid, 1993.

- **MURILLO DE LA CUEVA, P.L.:** "El derecho a la libertad informática", en la Base de conocimiento jurídico IUSTEL, www. Iustel.com

- **NAVAS NAVARRO, S.:** "Computación en la nube: Big Data y protección de datos personales", *InDret*, Barcelona, octubre 2015.

- **OROZCO PARDO** con cita a **PAULA SIBILA** en "Intimidad, privacidad, "extimidad" y protección de datos del menor. ¿Un cambio de paradigma", en **BOIX REIG, J. (Director), JAREÑO LEAL, A.** (Coordinador): *La protección jurídica de la intimidad*, Ed. Iustel, 1º Edición, Madrid 2010.

- **ORZA LINARES, R. M:** "Derechos fundamentales e Internet: nuevos problemas, nuevos retos", *ReDCE*. Año 9. Núm. 18. Julio-diciembre/2012. Págs. 275-336

- **PANIZA FULLANA, A.:** "Una nueva era en la privacidad y las comunicaciones electrónicas: La Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto a la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas", en *Revista Doctrinal Aranzadi Civil-Mercantil*, nº 7/2017, 2017.

- **PAZOS CASTRO, R.:** "El derecho al olvido frente a los editores de hemerotecas digitales: A propósito de la STS (Pleno de la Sala 1ª) de 15 de octubre de 2015". *InDret*, Barcelona, octubre 2016.

- **PÉREZ LUÑO, A.E.:** "Concepto y concepción de los derechos humanos", Doxa. Cuadernos de Filosofía del Derecho. Núm. 4, 1987.

- **PIAO HAU HSU:** "The Right to Be Forgotten and its ramifications in Taiwan, China and Japan", e-conference on the Right to be Forgotten in Europe and Beyond, June 2017, Blogdroiteuropeen; https://blogdroiteuropeen.com/2017/06/13/the-right-to-be-forgotten-and-its-ramifications-in-taiwan-china-and-japan-by-piao-hao-hsu/

- **PIÑAR MAÑAS, J.L.:** "Protección de datos, origen, situación real y retos de futuro" en *El Derecho a la autodeterminación informativa*, Fundación coloquio jurídico europeo, Ed. San José, Madrid, 2009. Págs. 81 a 179

- **PROSSER, W.:** "Privacy", *California Law Review*, 1960.

- **RIFKIN, J.:** "The Third Industrial Revolution: How the Internet, Green Electricity, and 3-D Printing are Ushering in a Sustainable Era of Distributed Capitalism" https://web.archive.org/web/20120331180815/http://www.worldfinancialreview.com/?p=1547

- **RODRÍGUEZ PALOP, M.E.:** "Antonio Enrique PÉREZ LUÑO: La tercera generación de derechos humanos, Aranzadi, Navarra, 2006, 315 pp."; *DERECHOS Y LIBERTADES; Número 16*, Época II, enero 2007, pp. 277-284

- **RODRIGO PICA, F.:** "El derecho fundamental al olvido en la web y el sistema constitucional chileno. Comentario a la sentencia de protección Rol Nº 22243-2015 de la Corte Suprema"; *Estudios Constitucionales, Año 14, Nº 1*, 2016, pp. 309-318; ISSN 07180195 https://scielo.conicyt.cl/pdf/estconst/v14n1/art10.pdf

- **ROMEO RUIZ, A.:** "El derecho al olvido en las administraciones públicas", *Revista española de derecho administrativo, nº 198*, 2019, págs. 215-242,

- **RUIZ MIGUEL, C.:** "El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea: análisis crítico". *Revista de Derecho Comunitario Europeo, año 7*, núm. 14, Enero-abril 2003.

- **SANCHEZ BRAVO, A.:** "Derecho a la Informática". *Base de conocimiento jurídico*, Ed. IUSTEL.

- **SÁNCHEZ GÓMEZ, A.,** "Los derechos fundamentales a la intimidad, honor y protección de datos en la era digital: mecanismos jurídicos de protección, carencias y retos del legislador: de las leyes de 1982 (LOPHII) y de 1999 (LOPD) al Reglamento europeo de protección de datos de 2016", *Revista de Derecho Privado*, núm. 100, 2016, págs. 77-125.

- **SALAS CLAVER, G.:** "Análisis comparativo de la propuesta del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos", *Certamen de artículos jurídicos sobre Derecho del entretenimiento 2015* Premios DENAE, Ed. DENAE, Madrid 2015.

- **SALDAÑA, M.N.:** "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis". *Revista de Derecho Político de la UNED*, N.º 85, septiembre-diciembre 2012, págs. 195-240.

- **SANTOS VENTOSA, G.:** "Hacía el reconocimiento del derecho al olvido en Iberoamérica", noviembre 2016;

https://ecija.com/wp-content/uploads/2016/11/Derecho_al_olvido_Iberoamerica.pdf

- **SCHIAVI, P.:** "El derecho al olvido y la protección de datos personales en Uruguay". Revista de derecho de la Universidad de Montevideo; Número 31 — año 2017; http://revistaderecho.um.edu.uy/wp-content/uploads/2017/09/SCHIAVI-Pablo-El-derecho-al-olvido-y-a-la-proteccion-de-datos-personales-en-Uruguay.pdf

- **SELMA PENALVA, A.:** "La información reflejada en las redes sociales y su valor como prueba en el proceso laboral. Análisis de los últimos criterios jurisprudenciales". *Revista General de Derecho del Trabajo y de la Seguridad Social núm. 39*, Ed. IUSTEL. Madrid 2014.

- **SORIANO GARCÍA, J.E.:** "Presente del derecho al olvido". El Cronista del Estado Social y Democrático de Derecho, ISSN 1889-0016, Nº. 78, 2018, págs. 4-21.

- **TOSCANO GIL, F:** "Publicación de actos administrativos y protección de datos de carácter personal". *Revista General de Derecho Administrativo* núm. 31, Ed. Iustel, Madrid 2012.

- **TAMBÚ, O.:"** Le Droit à l'oubli en Europe et au-delà"; abril 2018; 408024; Centre de recherche Droit Dauphine [Cr2D]; Universitè de Paris.

- **VV.AA. NATO Review** / The "Lisa case": Germany as a target of Russian disinformation;

https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm

- **VESTO, A.:** "La tutela dell'oblio tra intimità e condivisione senza filtri". *Rivista di diritto dei media*. 2/2018.

- **VILLAVERDE MENÉNDEZ, I.,** "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo: a propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, núm. 41, 1994, págs. 173-187.

- **VOLOKH, E:** "Google: First amendment protection for Search Engine Results", published version of a White Paper commissioned by Google: http://www2.law.ucla.edu/volokh/searchengine.pdf

- **WARREN, S. y BRANDEIS, L.:** "The Right to privacy", en *Harvard Law Review*, Vol. IV, 15 de diciembre de 1890, núm. 5. http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

  También en Cuadernos Cívitas "El derecho a la intimidad", edición al cargo de Benigno PENDAS y Pilar BASELGA, Ed. Cívitas, S.A., Madrid, 1995.

3. LEGISLACIÓN:

- Petition rights

- Bill of Rights

- Declaración de Independencia Norteamericana

- Declaración de Derechos del buen pueblo de Virginia de 1776

- Declaración Francesa de los Derechos del Hombre y del Ciudadano en el año 1789

- Declaración Americana de Derechos y Deberes del Hombre http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp

- Declaración Universal de los Derechos Humanos http://www.un.org/es/universal-declaration-human-rights/

- Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales de 1950 https://www.echr.coe.int/Documents/Convention_SPA.pdf

- Pacto internacional de los derechos civiles y políticos de 1966 https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx

- Constitución Española de 27 de diciembre de 1978 (BOE 29/12/1978)

- Código Civil, de 24 de julio de 1889

- Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. BOE» núm. 262, de 31 de octubre de 1992, páginas 37037 a 37045.

- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos. Publicado en: «BOE» núm. 106, de 4 de mayo de 1993, páginas 13244 a 13250

- Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Publicado en: «BOE» núm. 147, de 21 de junio de 1994, páginas 19199 a 19203

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. Publicado en: «BOE» núm. 151, de 25 de junio de 1999, páginas 24241 a 24245.

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (BOE 24/11/1995; corr. err. BOE 2/03/1996, BOE 29/01/2011)

- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, BOE núm. 298 de 14 de diciembre de 1999.

- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, BOE núm. 106, de 04/05/1993.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. BOE núm. 301, de 16 de diciembre de 2000, páginas 44253 a 44257 https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726

- Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones. BOE núm. 4 de 5 de enero de 2005. https://www.boe.es/boe/dias/2005/01/05/pdfs/A00280-00281.pdf

- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. «BOE» núm. 296, de 12/12/2006 https://www.boe.es/buscar/act.php?id=BOE-A-2006-21648

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE» núm. 17, de 19/01/2008. https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid; BOCM de 25 de Julio de 2001

- Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas de la CAM; BOCM de 29 de diciembre de 2012, Corrección de errores: (BOCM de 15 de Enero de 2013)

- Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos

Publicado en DOGC núm. 3625 de 29 de Abril de 2002 y BOE núm. 115 de 14 de Mayo de 2002

- Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, «DOGC» núm. 5731, de 08/10/2010, «BOE» núm. 257, de 23/10/2010
  https://www.boe.es/buscar/act.php?id=BOE-A-2010-16136

- Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos; BOPV» núm. 44, de 4 de marzo de 2004, «BOE» núm. 279, de 19 de noviembre de 2011
  https://www.boe.es/buscar/pdf/2011/BOE-A-2011-18151-consolidado.pdf

- Decreto 308/2005, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos
  Boletín Oficial del Pais Vasco de 16-11-2005

- Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía; BOJA nº 124 de 30/06/2014
  https://www.juntadeandalucia.es/boja/2014/124/1

- Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía. BOJA nº 193 de 02/10/2015
  https://www.juntadeandalucia.es/boja/2015/193/1

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, «BOE» núm. 166, de 12/07/2002.
  https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

- Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero
  «BOE» núm. 281, de 23/11/2002
  https://www.boe.es/buscar/act.php?id=BOE-A-2002-22807

- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, «BOE» núm. 114, de 10/05/2014.
  https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950

- Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras; «BOE» núm. 168, de 15/07/2015.
  https://www.boe.es/buscar/act.php?id=BOE-A-2015-7897

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
  https://www.boe.es/buscar/act.php?id=BOE-A-2015-10566&p=20151002&tn=2

- Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y propia imagen. «BOE» núm. 115, de 14/05/1982
  https://www.boe.es/buscar/act.php?id=BOE-A-1982-11196

- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. «BOE» núm. 285, de 27/11/1992.

https://www.boe.es/buscar/act.php?id=BOE-A-1992-26318

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, Diario Oficial n° L 281 de 23/11/1995 p. 0031 – 0050
  https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A31995L0046

- Carta de los derechos fundamentales de la Unión Europea (2000/C 364/01); publicado en el Diario Oficial de las Comunidades Europeas de 18.12.2000
  http://www.europarl.europa.eu/charter/pdf/text_es.pdf

- Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea - Diario Oficial n° C 326 de 26/10/2012 p. 0001 – 0390
  https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12012E%2FTXT

- Directiva sobre la privacidad y las comunicaciones electrónicas (2002/58/CE)
  https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32002L0058

- Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (DO C 306 de 17.12.2007), ratificado por España el veintiséis de septiembre de dos mil ocho
  https://www.boe.es/buscar/doc.php?id=BOE-A-2009-18898

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos) (Texto pertinente a efectos del EEE)
https://eur-lex.europa.eu/legal-ontent/ES/ALL/?uri=CELEX:32016R0679

- Alemania: Act to Adapt Data protection Law to regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680
http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/44.pdf

- DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo
https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L0680&from=EN

- REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las electrónicas) COM/2017/010 final - 2017/03 (COD)
https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

- PROPOSITION DE LOI, visant à définir et sanctionner les fausses nouvelles ou « fake news »,
  https://www.senat.fr/leg/ppl16-470.html

- Ley n° 78-17 de 6 de enero 1978 relativa a la informática, los ficheros y las libertades
  https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

- Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique
  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id

- Lei n.° 67/98 de 26 de Outubro (Dados pessoais)
  http://www.wipo.int/wipolex/es/text.jsp?file_id=206648

- Ley 58/2019, por la que se garantiza la aplicación, en el ordenamiento jurídico nacional, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
  https://dre.pt/web/guest/home/-/dre/123815982/details/maximized

- UK: Data Protection Bill
  http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/49.pdf

- Netzdurchsetzunggesetz, NetzDG
  https://germanlawarchive.iuscomp.org/?p=1245

- California Senate Bill No. 568: Privacy Rights for California Minors in the Digital World https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568

4. JURISPRUDENCIA:

A. JURISPRUDENCIA DEL TRIBUNAL EUROPEO DE DERECHOS HUMANOS

- STEDH M.L y W.W c./ Alemania, de 28 de junio de 2018
- STEDH Niemietz contra Alemania de 16 diciembre 1992, serie A núm. 251
- STEDH S. y Marper v. Reino Unido [GC], núm. 30562/04 y 30566 / 04, § 41, de 4 de diciembre de 2008
- STEDH Rotaru v. Rumania [GC], §§ 43-44).
- STEDH Amann v. Suiza [GC], §§ 65-67 ;
- STEDH Leander c. Suecia, § 48 ; Kopp c. Suiza, § 53)
- STEDH M.N. y otros v. San Marino, § 51
- STEDH G.S.B. v. Suiza, § 93
- STEDH Asociación "21 de diciembre 1989" y otros c. Rumanía, § 115
- STEDH Gardel c. Francia, § 58
- STEDH M.K. c. Francia
- STEDH Federación nacional y sindicatos deportivos (FNASS) y otros contra Francia, §§ 155-159
- STEDH Segerstedt-Wiberg y otros contra Suecia, § 88
- STEDH Murray c. Reino Unido, § 93
- STEDH M.M. c. Reino Unido, § 199
- STEDH Van der Velden c. Países Bajos (déc.);
- STEDH W. c. Países Bajos (déc.)),
- STEDH Peruzzo et Martens c. Alemania (déc.), §§ 42 et 49).
- STEDH Aycaguer c. Francia
- STEDH Caruana c. Malta

- STEDH Satakunnan Markkinapörssi Oy y Satamedia Oy c. Finlandia [GC], § 133
- STEDH Leander c. Suecia, § 48; Rotaru c. Rumanía [GC], § 46
- STEDH Z c. Finlandia, § 95
- STEDH B.B. c. Francia, § 60
- STEDH M.B. c. Francia, § 62
- STEDH Sõro v. Estonia, §§ 56-64
- STEDH Ivanovski la ex República Yugoslava de Macedonia, § 176
- STEDH Anchev v. Bulgaria
- STEDH Couderc y Hachette Filipacchi Associés v. Francia [GC], § 91,
- STEDH Medžlis Islamske Zajednice Brčko y otros Bosnia y Herzegovina [GC], § 77).
- STEDH Von Hannover v. Alemania (no. 2) [GC], §§ 108-113;
- STEDH Axel Springer AG v. Alemania [GC], §§ 89-95).
- STEDH Tamiz c. Reino Unido

B./ JURISPRUDENCIA CONSTITUCIONAL:

- STC 73/1982
- STC 105/1983
- STC 110/1984,
- STC 107/1987
- STS de 23 de marzo de 1987
- STC 165/1987
- STC, asunto Crespo Martínez, de 21 de enero de 1988.
- STC 6/1988;
- STC 107/1988, de 8 de junio

- STC 231/1988, de 2 de diciembre
- STC 217/1989, de 21 de diciembre.
- STC 105/1990;
- STC 171/1990;
- STC 197/1991, de 17 de octubre;
- STC 240/1992
- STC 32/1994, de 31 de enero;
- STC 57/1994, de 18 de febrero;
- STC 143/1994, de 9 de mayo;
- STC 138/1996, de 16 de septiembre,
- STC 207/1996, de 16 de diciembre;
- STC 151/1997
- STC 204/1997
- STC 144/1998, de 30 de julio,
- STC 134/1999 de 15 de julio
- STC 144/1999 de 22 de julio
- STC 21/2000, de 31 de enero,
- STC 112/2000, de 5 de mayo,
- STC 290/2000, de 30 de noviembre
- STC 292/2000, de 30 de noviembre
- STC 14/2001, de 29 de enero
- STC 202/2001, de 21 de noviembre,
- STV 81/2.001, de 26 de marzo
- STC 156/2001, de 2 de julio;
- STC 20/2002, de 28 de enero
- STC 76/2002, de 8 de abril,
- STC 83/2.002, de 22 de abril
- STC 127/2003, de 30 de junio,

- STC 160/2003, de 15 de septiembre
- STC 61/2004, de 19 de abril.
- STC 151/2004, de 20 de septiembre
- STC 196/2004, de 15 de noviembre
- STC 104/2006, de 3 de abril.
- STC 9/2007, de 15 de enero
- STC 129/2009, de 1 de junio
- STC 41/2011, de 11 de abril
- STC 4/2018, de 4 de junio de 2018, dictada en el recurso de amparo 2096/2016
- STC 76/2019, de 22 de mayo.

C./ JURISPRUDENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

- Sentencia del Pleno del TJUE, de 6 de noviembre 2003, asunto C-101/2001 (Caso Lindqvist)

- Sentencia del Tribunal de Justicia de la Unión Europea, de 23 de marzo de 2010, asuntos acumulados C-236/08 a C-238/08 (Caso Louis Vuitton)

- Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014, en el asunto C-131/12, Google España, S.L., Google, Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González.

- Conclusiones del Abogado General, Sr. NIILO JÄÄSKINEN, presentadas el 25 de junio de 2013, en el asunto C-131/12, Google

España, S.L., Google, Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González.

- Sentencia del TJUE de 9 de marzo de 2017, en el asunto C-398/15, Salvatore Manni. http://curia.europa.eu/juris/document/document.jsf?text=&docid=188750&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=9111226

- Solicitud de cuestión prejudicial elevada por el Consejo de Estado francés al Tribunal de Justicia de la Unión Europea el 19 de julio de 2017 sobre el alcance territorial del derecho de desindexación CE, 19 juillet 2017, GOOGLE INC. N° 399922 http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC

- Conclusiones abogado General asunto C-507/17; SR. MACIEJ SZPUNAR presentadas el 10 de enero de 2019: http://curia.europa.eu/juris/document/document.jsf?text=&docid=209688&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=1864979

- Sentencia del TJUE de 24 de septiembre de 2019, el asunto C-507/17: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=9112699

- Sentencia del TJUE; de 24 de septiembre de 2019 en el asunto C-137/17, GC, AF, BH, ED, CNIL, Premier ministre, Google LLC. http://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=9114099

D./ SENTENCIAS DEL TRIBUNAL SUPREMO DE ESPAÑA

Sentencias Sala Tercera del Tribunal Supremo

- STS núm. 1611/2016 de 4 julio
- STS de 11 de marzo -recursos 643/2015 (RJ 2016, 1519)
- STS 1482/2015 (RJ 2016, 1519), 14 de marzo -recursos 1078/2015 (RJ 2016, 1525)
- STS 1380/2015 (RJ 2016,1071), 15 de marzo de 2016 (RJ 2016, 1301)-recurso 804/2015
- ATS de 31 de mayo de 2019 (RCA 1074/2019,
- STS n.º 1917/2016, de 21 de julio (RCA 2866/2015)-
- STS nº. 12/2019, de 11 de enero (RCA 5579/2017)-; o la
- STS n.º 1407/2018, de 20 de septiembre (RCA 2828/2016

Sentencias de la Sala Primera del Tribunal Supremo:

- Sentencia del Pleno de la Sala de lo civil del Tribunal Supremo de 15 de octubre de 2015, dictada en el Recurso de casación núm. 2772/2013

- Sentencia núm. 210/2016 de 5 abril, del Pleno de la Sala de lo Civil del Tribunal Supremo, que confirma otra de la Audiencia provincial de Barcelona

E./ SENTENCIAS DE LA AUDIENCIA NACIONAL

- Auto de fecha 27 de febrero de 2012, núm. 19/2012, la Audiencia Nacional: a través del cual se formula petición de decisión prejudicial presentada por la Audiencia Nacional (España) el 9 de marzo de 2012 — Google España, S.L., Google, Inc./Agencia de Protección de Datos (AEPD), Mario Costeja González

- Sentencia de la Sala de lo contencioso-administrativo de la Audiencia Nacional (Sección 1ª), de 21 de junio de 2019, dictada en el recurso núm: 106/2018

- Sentencia también de 21 de junio de 2019 dictada en el recurso núm. 217/2018

- Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 21 de junio de 2019, en el recurso 215 / 2018

- Sentencia de 16 de mayo de 2019, de la Sección 1ª de la Sala de lo contencioso administrativo de la Audiencia Nacional, en el recurso 609/2017

- Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 9 de mayo de 2019, en el recurso 491/2017

- Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 22 de abril de 2019 en el recurso núm. 343/2017

- Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, en el recurso 528/2017, de 2 de abril de 2019

- Sentencia de la Sección 1ª de la Sala tercera de la Audiencia Nacional, de 26 de marzo de 2019 en el recurso núm. 468/2017

- Sentencia de la Sala de lo contencioso-administrativo de la Audiencia Nacional, de 29 de diciembre de 2014, dictada en el recurso núm. 725/2010. Ponente: De Mateo Menéndez, Fernando.

F./ SENTENCIAS AUDIENCIAS PROVINCIALES:

- Sentencia de 17 de julio de 2014, dictada por la Audiencia Provincial de Barcelona (sección 16ª), en el rollo de apelación nº 99/2012, dimanante de los autos de juicio ordinario nº 411/2011 del Juzgado de primera instancia nº 8 de Barcelona

- Sentencia de 11 de octubre de 2013, dictada por la Sección 14ª de la Audiencia Provincial de Barcelona (rollo 486/2013),

G./ SENTENCIAS TRIBUNALES EXTRANJEROS:

- U.S. Supreme Court; Boyd v. United States, 116 U.S. 616 (1886)

- Higher Regional Court (Oberlandesgericht) Köln, I-15 U 197/15

- Sentencia de la Corte de apelación de Lieja 2013/RG/393, 25 de septiembre de 2014

- Sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre 1983. Ley del Censo. Derecho a la personalidad y dignidad humana

- Sentencia núm. 5525/2012 de la Corte de Casación italiana, de 5 de abril de 2012

- Tribunal de Roma se ha pronunciado sobre la cuestión del derecho al olvido en la Sentencia de la Sala de lo Civil, de 3 de diciembre de 2015, n. 23771

- Tribunal Regional Superior de Colonia I-15 U 197/15

- Sentencia de la Corte de apelación de Lieja 2013/RG/393, 25 de septiembre de 2014

- Corte de primera instancia de Estocolmo fallo a favor de Google, en una Sentencia de 9 de mayo de 2016

- Tribunal Supremo de Inglaterra y Gales se produjeron en abril de 2018,

- Sentencia del Tribunal Supremo de Canadá, A.T. c. Globe24h.com, 2017 CF 114

- Tercera Sala de la Corte Suprema de Chile proclamó por primera vez en ese país, mediante la Sentencia de fecha 21 de enero de 2016

- Sentencia de la Corte Constitucional de Colombia T-414/92

- Sentencia de la Corte Constitucional de Colombia T-277/15

- Sentencia de 31 de enero de 2017, del Tribunal Supremo de Japón

- Civil Judgment of People's Court of Haidian District, Beijing, No. (2015)Hai Min Chu 17417

H./ RESOLUCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS:

- Resolución Nº: R/00301/2019, Expediente Nº: TD/00111/2019;
- Resolución Nº: R/00297/2019, Expediente Nº: TD/00109/2019;
- Resolución Nº: R/00204/2019, Expediente Nº: TD/00059/2019).
- Resolución Nº: R/00307/2019; Expediente Nº: TD/00103/2019;
- Resolución nº: R/00290/2019, Expediente Nº: TD/00106/2019;
- Resolución Nº: R/00091/2019, dictada en el expediente Nº: TD/00068/2019).

- Resolución Nº: R/00218/2019, Expediente Nº: TD/00067/2019;
- Resolución Nº: R/00193/2019, Expediente Nº: TD/00028/2019;
- Resolución Nº: R/00146/2019, Expediente Nº: TD/00024/2019.

I./ RESOLUCIONES AGENCIAS DE PROTECCION DE DATOS EXTRANJERAS:

Francia:

- Resolución del CNIL de fecha de 10 de marzo de 2016, por la que se impone a Google una multa de 100.000 € por haberse negado a acatar la decisión anterior de la Comisión Nacional de la informática y de las libertades (CNIL), de 21 de mayo de 20154.733

Perú:

- Resoluciones agencia peruana de protección de datos:
- Resolución Directoral N° 045-2015-JUS/DGPDP de fecha 30 de diciembre de 2015.
- Resolución Directoral N° 026-2016-JUS/DGPDP de fecha 11 de marzo de 2016

Costa Rica:

- Resolución NO. 03 de la PRODHAB, en el Expediente 074-12-2015-DEN, de 18.2.2016;

- Resolución NO. 04 de la PRODHAB, en el EXPEDIENTE: 029-06-2016-DEN, de 2.09.2016;
- Resolución NO. 03 de la PRODHAB en el EXPEDIENTE: 040-06-2015-DEN, de 7.08.2015)

5. INFORMES, CONSULTAS PÚBLICAS, CONFERENCIAS Y DICTÁMENES:

- **PUENTE ESCOBAR, A.:** "Informes y sentencias relevantes", 7ª Sesión Anual abierta de la Agencia Española de Protección de Datos.

- **PUENTE ESCOBAR, A.:** "Informes y sentencias relevantes", 8ª Sesión Anual abierta de la Agencia Española de Protección de Datos. https://www.aepd.es/agencia/transparencia/jornadas/common/8-sesion/03-Agustin-Puente.pdf

- **PUENTE ESCOBAR, A.:** "Informes y sentencias relevantes", 9ª Sesión Anual abierta de la Agencia Española de Protección de Datos. https://www.aepd.es/agencia/transparencia/jornadas/common/9-sesion/04-Agustin-Puente.pdf

- **PUENTE ESCOBAR, A.:** "El Proyecto de Ley Orgánica de Protección de datos". 10ª Sesión Anual abierta de la Agencia Española de Protección de Datos. https://www.aepd.es/agencia/transparencia/jornadas/common/10-sesion/8-agustin-puente.pdf

- **WEEDON, J., NULAND, W., STAMOS, A.:** "Information Operations and Facebook", abril 2017. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

- Sumario de respuestas a la consulta pública sobre el futuro marco legal para la protección de datos

https://ec.europa.eu/home-affairs/what-is-new/public-consultation/2009/consulting_0003_en

- Grupo de trabajo del art. 29 (WP-225): "GUIDELINES ON THE IMPLEMENTATION OF THE COURT OF JUSTICE OF THE EUROPEAN UNION JUDGMENT ON "GOOGLE SPAIN AND INC V. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ" C-131/12", 26.11.2014

- The Advisory Council to Google on the Right to be forgotten, 6. Feb. 2015. https://static.googleusercontent.com/media/archive.google.com/es//advisorycouncil/advisement/advisory-report.pdf

- SPEECH/12/26; **Viviane Reding;** Vice-President of the European Commission, EU Justice Commissioner; "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones; Un enfoque global de la protección de los datos personales en la Unión Europea, de 4.11.2010 https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC0609&from=ES

- Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — «Un enfoque global de la protección de los datos personales en la Unión Europea» (2011/C 181/01)

https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_es.pdf

- Resolución del Parlamento Europeo de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea (2011/2025(INI)
  http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//ES

- Posición del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos).
  https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_5419_2016_REV_1&from=EN

- Comunicación de la Comisión al Parlamento y al Consejo, con Orientaciones sobre la aplicación directa de ese Reglamento General de protección de datos, publicada el 24 de enero de 2018.
  https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0043&qid=1517578296944&from=EN

- Comunicación de la Comisión al Parlamento Europeo y al Consejo, al Comité económico y social europeo y al Comité de las regiones "La Construcción de una Economía de los datos europea". 10.1.2017
  http://ec.europa.eu/transparency/regdoc/rep/1/2017/ES/COM-2017-9-F1-ES-MAIN-PART-1.PDF

- Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online, AEPD y Instituto Nacional de Tecnologías de la Comunicación
https://www.uv.es/limprot/boletin9/inteco.pdf

- Council of Europe: INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making;
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

- Consulta pública sobre noticias falsas y desinformación en línea
https://ec.europa.eu/info/consultations/public-consultation-fake-news-and-online-disinformation_es

- Summary report of the public consultation on fake news and online disinformation
https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-fake-news-and-online-disinformation

- Parlamento Europeo, 3 a 6 de abril de 2017: "Incitación al odio, populismo y noticias falsas - debate en el pleno"
http://www.europarl.europa.eu/news/es/agenda/briefing/2017-04-03/6/incitacion-al-odio-populismo-y-noticias-falsas-debate-en-el-pleno

- Resolución del Parlamento Europeo, de 15 de junio de 2017, sobre las plataformas en línea y el mercado único digital
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0272+0+DOC+XML+V0//ES

- Propuesta de Resolución del Parlamento Europeo sobre el nuevo grupo de trabajo europeo contra las noticias falsas (fake news); 31.8.2017 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-2017-0501+0+DOC+XML+V0//ES

- 12.3.2018; Final results of the Eurobarometer on fake news and online disinformation https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation

- 12.3.2018; Final report of the High Level Expert Group on Fake News and Online Disinformation https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

- Joint research Center/European Comission: The digital transformation of news media and the rise of disinformation and fake news, Abril 2018; https://ec.europa.eu/jrc/sites/jrcsh/files/jrc111529.pdf

- CE, 19 juillet 2017, GOOGLE INC. N° 399922 http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC

- Informe de la Asamblea Nacional sobre el impacto del RGPD de la UE sobre la legislación francesa http://www.congreso.es/docu/docum/ddocum/dosieres/sleg/legislatura_12/spl_13/pdfs/48.pdf

- Guida del Garante per la protezione dei dati personali all applicazione del Regolamento UE 2016/679
https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf

- DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS; Año 2018 XII LEGISLATURA Núm. 104; Sesión plenaria núm. 99, celebrada el jueves, 15 de febrero de 2018
http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28DSCD-12-PL-104.CODI.%29#(P%C3%A1gina28)

- Informe de la ponencia sobre el Proyecto de Ley Orgánica de protección de datos: BOLETÍN OFICIAL DE LAS CORTES GENERALES; CONGRESO DE LOS DIPUTADOS; XII LEGISLATURA; SERIE A: PROYECTOS DE LEY; 9 DE OCTUBRE DE 2018
http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&DOCORDER=LIFO&QUERY=%28BOCG-12-A-13-3.CODI.%29#(P%C3%A1gina1)

6. ARTÍCULOS DE PRENSA:

- **AGENCIAS:** "Los 28 aprueban la normativa de protección de datos que reconoce el derecho al olvido"; El confidencial; 15.06.2015 http://www.elconfidencial.com/tecnologia/20150615/los28apruebanlanormativadeprotecciondedatosquereconoceelderechoalolvido_882079/

- **AGENCIAS:** "Los españoles somos los europeos que más nos creemos las mentiras de las fake news"; Diario La Razón, 11.09.2018 https://www.larazon.es/tv-y-comunicacion/media-news/los-espanoles-somos-los-europeos-que-mas-nos-creemos-las-mentiras-de-las-fake-news-PA19801428

- **AGENCIAS:** "Euskadi recibe más de 800 consultas sobre protección de datos". https://www.noticiasdegipuzkoa.eus/2018/07/16/sociedad/euskadi-recibe-mas-de-800-consultas-sobre-proteccion-de-datos

- **ALANDETE, D.:** "Un grupo de eurodiputados se moviliza para impulsar una legislación sobre noticias falsas"; El país, 17.04.2018 https://elpais.com/internacional/2018/04/15/actualidad/1523786863_641545.html

- **ALANDETE, D.:** "La UE combate la máquina de propaganda del Kremlin", Diario El País, 10/11/2017 https://elpais.com/politica/2017/11/08/actualidad/1510166614_571653.html

- **ALDEA, M.; BALIBREA, A.; GALLEGO NICASIO, L.; GONZÁLEZ, M.; HURTADO, A.; RODRIGO, M. J.; TOURIÑO, A.; ZÁRATE, C.:** "Guías legales sobre Internet: derecho de las tecnologías de la información y la comunicación en entornos empresariales, Expansión, sábado 27 de febrero de 2016.

- **ALZUETA, L. y otros:** "Guías legales sobre Internet: tecnologías en el trabajo: privacidad y productividad", Expansión, sábado 12 de marzo de 2016.

- **AMANN, M., BECKER, M., BIDDER, B.:** "Russia's Propaganda Campaign Against Germany", en Spiegel, [interactivo], 2016 http://www.spiegel.de/international/europe/putin-wages-hybrid-war-on-germany-and-west-a-1075483.html

- **BASSETS, M.:** "Macron anuncia una ley contra las noticias falsas", El País, 4 de enero de 2018. https://elpais.com/internacional/2018/01/03/actualidad/1515002815_273219.html

- **BLANCO, A.:** "Google rechaza el 41% de las peticiones de "derecho al olvido" de los españoles"; El confidencial; 21.07.2015 http://www.elconfidencial.com/tecnologia/20150721/derechoalolvidogooglespanapeticiones_935888/

- **CARIA, J:** 19.10.2018, http://exameinformatica.sapo.pt/noticias/mercados/2018-10-19-CNPD-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos www.exameinformatica.sapo.pt

- **CARRILLO, I y otros:** "Guías legales sobre Internet: derecho en Internet para particulares", Expansión, sábado 5 de marzo de 2016.

- **CARRILLO, M.:** "El 'derecho al olvido' no es absoluto", EL País, 27/02/2013

- **CARRILLO, M:** "El derecho al olvido en Internet", El País, 26.10.2009

- **CEBERIO.M., GÓMEZ, R.G.:** ¿Decidirá Google lo que es verdad?, Diario El País, 3.4.2018

- **CONFILEGAL:** "Alemania endurecerá la ley contra Facebook: 500.000 euros por publicar noticias falsas y mensajes de odio"; 20.12.2016 https://confilegal.com/20161220-alemania-se-pone-dura-facebook/

- **EFE:** "Juncker insta a actuar con contundencia ante las falsas noticias en Internet", 26.12.2016 https://www.efe.com/efe/america/portada/juncker-insta-a-actuar-con-contundencia-ante-las-falsas-noticias-en-Internet/20000064-3134031

- **EUROEFE:** ""Fake news" y cómo la UE lucha contra la desinformación"; 5.4.2018; http://euroefe.euractiv.es/5533_dosieres/5271307_fake-news-y-como-la-ue-lucha-contra-la-desinformacion.html

- **EUROPAPRESS:** "Mogherini pide a los Gobiernos europeos más recursos para atajar la propaganda y desinformación rusa"; 13/11/2017

https://www.europapress.es/internacional/noticia-mogherini-pide-gobiernos-europeos-mas-recursos-atajar-propaganda-desinformacion-rusa-20171113113831.html

- **EUROPAPRESS:** "El grupo de expertos en 'fake news' designado por Bruselas reclama mayor transparencia a las plataformas en línea", 12/3/2018 https://www.europapress.es/sociedad/noticia-grupo-expertos-fake-news-designado-bruselas-reclama-mayor-transparencia-plataformas-linea-20180312180149.html

- **FEDERACIÓN DE ASOCIACIONES DE PERIODISTAS DE ESPAÑA (FAPE):** "La FAPE rechaza la comisión de control sobre "noticias falsas" y pide transparencia", 18.12.2017 http://fape.es/la-fape-rechaza-la-comision-de-control-sobre-noticias-falsas-y-pide-transparencia/?_ga=2.118976522.24367327.1538047702-1440417349.1538047702

- **GIBBS, S.:** "EU to Google: expand 'right to be forgotten' to Google.com", The Guardian, 27.11.2014; http://www.theguardian.com/technology/2014/nov/27/eutogoogleexpandrighttobeforgottentogooglecom

- **GIBBS, S.:** "French data regulator rejects Google's rightto-be-forgotten appeal", The Guardian, 27.09.2015; http://www.theguardian.com/technology/2015/sep/21/frenchgooglerighttobeforgottenappeal

- **GIBBS, S.:** Google ordered to remove links to 'right to be forgotten' removal stories", The Guardian, 20.8.2015;

http://www.theguardian.com/technology/2015/aug/20/googleorderedtoremovelinkstostoriesaboutrighttobeforgottenremovals

- **GOEL, V. y otros:** "En India los rumores de WhatsApp matan", New York Times, 24.7.2018; https://www.nytimes.com/es/2018/07/24/whatsapp-rumores-violencia-india/

- **GÓMEZ FUENTES, A.:** "Alarma en Italia sobre la invasión de las fake news": Diario ABC, 29.11.2017; https://www.abc.es/internacional/abci-alarma-italia-sobre-invasion-fake-news-201711271505_noticia.html

- **GÓMEZ RUIZ, L.:** "Fake news", la palabra del año según el Diccionario Oxford"; lA VANGUARDIA: 7/11/2017 https://www.lavanguardia.com/cultura/20171107/432683218631/fake-news-palabra-ano-diccionario-oxford.html

- **GRIERSON, J., QUEEN, B.:** "Google loses landmark 'right to be forgotten' case", The Guardian, 13.4.2018; https://www.theguardian.com/technology/2018/apr/13/google-loses-right-to-be-forgotten-case

- **HOROWITZ, J.:** "In Italian Schools, Reading, Writing and Recognizing Fake News", The New York Times, 18.10.2017 https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html?_r=0

- **KISS, J.:** "Dear Google: open letter from 80 academics on 'right to be forgotten', The Guardian, 14.5.2015; http://www.theguardian.com/technology/2015/may/14/deargoogleopenletterfrom80academicsonrighttobeforgotten

- **KISS, J.:** "Google must be more open on 'right to be forgotten', academics warn in letter", The Guardian, 14.5.2015 http://www.theguardian.com/technology/2015/may/14/googlerighttobeforgottenacademicsletter

- **LANTIGUA, I.:** ¿Qué debe hacer alguien que quiera ejercer su 'derecho al olvido'?; 20/10/2015; Diario El Mundo; http://www.elmundo.es/sociedad/2015/10/20/5625509422601d1d478b4664.html

- **LÓPEZ, E.:** "Derecho al olvido en la red", Diario La Razón, 8 de agosto de 2011.

- **LUNA, A.G.:** "La Audiencia Nacional respalda la decisión de la UE: el derecho al olvido llega a España; El confidencial; 23.01.2015; http://www.elconfidencial.com/tecnologia/20150123/laaudiencianacionalrespaldaladecisiondeeuropayratificaelderechoalolvido_628735/

- **MARRACO, M.:** "Derecho al olvido: datos ocultos pero imborrables"; 19.10.2015 http://www.elmundo.es/tecnologia/2015/10/19/56250abf22601dee298b4624.html

- **MARTÍNEZ MARTÍNEZ, R.:** "Diseñar el derecho al olvido"; diario ABC, 29.11.2012

- **MATEO, J.J.:** El País, 19/09/2017: "La Agencia de Protección de Datos investiga un posible acceso ilícito para crear el censo electoral catalán"

  https://elpais.com/politica/2017/09/18/actualidad/1505734999_480220.html

- **PARRONDO, N.:** "Un estudio explica por qué las 'fake news' son más seductoras que la verdad", Revista GQ México; 9.03.2018
  https://www.gq.com.mx/actualidad/articulos/fake-news-verdad-mit-estudio/10702

- **PAYUETA, E.:** "Guía para identificar las fake news"; Diario El Mundo, Impulso digital;
  http://www.impulsodigital.elmundo.es/seguridad-tecnologica/guia-para-identificar-las-fake-news

- **PELLICER, Ll.:** "La justicia europea da la razón a Google y limita el derecho al olvido a la UE, Diario El País, 24 de septiembre de 2019.
  https://elpais.com/sociedad/2019/09/24/actualidad/1569314265_134650.html

- **PÉREZ-LANZAC, C.:** "El Supremo deriva el "derecho al olvido" a la central del Google", Diario El País, 15 de marzo de 2016.

- **PIÑAR MAÑAS, J.L.**; "Derecho al olvido, a saber y al propio pasado"; diario El Mundo; 9.9.2014.

- **PIQUÉ, E.:** "Educación para combatir el peligroso fenómeno de las fake news", La Nación, 9 de noviembre de 2017; https://www.lanacion.com.ar/2080689-educacion-para-combatir-el-peligroso-fenomeno-delas-fake-news

- **POWLES, J.:** "Right to be forgotten: Swiss cheese Internet, or database of ruin?", The Guardian, 1.8.2015; http://www.theguardian.com/technology/2015/aug/01/righttobeforgotten googleswisscheeseInternetdatabaseofruin

- **R.GG/ M.C.B:** "64.000 españoles quieren ser olvidados", Diario El País, 3.4.2018

- **RIFKIN, J.:** "The Third Industrial Revolution: How the Internet, Green Electricity, and 3-D Printing are Ushering in a Sustainable Era of Distributed Capitalism" https://web.archive.org/web/20120331180815/http://www.worldfinancialreview.com/?p=1547

- **RINCÓN, R.**: "Dos salas del Tribunal Supremo discrepan sobre el 'derecho al olvido'"; 6.4.2016; http://politica.elpais.com/politica/2016/04/06/actualidad/1459970204_096387.html

- **RODRIGUEZ, C.:** "Fake news", palabra del año del Diccionario Oxford"; EL MUNDO; 7/11/2017: http://www.elmundo.es/cultura/cine/2017/11/03/59fc80f4468aebd1508b46a0.html

- **ROUCO, F.** "Las Noticias falsas son solo la superficie del problema": https://telos.fundaciontelefonica.com/noticias-falsas-problema-fake-news/

- 25.01.2015; http://www.derechoolvido.es/la-corte-suprema-de-chile-publica-una-sentencia-sobre-el-derecho-al-olvido/

- **SCHECHENER, S.:** "EU Opposes France on Global 'Right to Be Forgotten'"; The Wall Street Journal, Sept. 11, 2018; https://www.wsj.com/articles/eu-executive-arm-opposes-france-on-global-right-to-be-forgotten-1536685575

- **SOLOZABAL, J.J.:** "La privacidad y sus riesgos", El imparcial, 30.10.2018 https://www.elimparcial.es/noticia/195154/opinion/la-privacidad-y-sus-riesgos.html

- **TIPPMANN S., POWLES, J.:** "Google accidentally reveals data on 'right to be forgotten' requests"; The Guardian; 14.07.2015 http://www.theguardian.com/technology/2015/jul/14/googleaccidentallyrevealsrighttobeforgottenrequests

ANEXO I

ANEXO 1.- COMPARATIVO REDACCIÓN ART. 17 RGPD; COMISIÓN EUROPEA- PARLAMENTO EUROPEO-CONSEJO

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos) /* COM/2012/011 final - 2012/0011 (COD) */ https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012PC0011&from=EN	Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de datos) (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD))(Procedimiento legislativo ordinario: primera lectura)(2017/C 378/55) https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52014AP0212&from=EN	Posición del Consejo en primera lectura con vistas a la adopción de un REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_5419_2016_REV_1&from=EN
Artículo 17 **Derecho al olvido y a la supresión** 1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes: a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19; d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos.	**Artículo 17** **Derecho ~~al olvido y~~ a la supresión** 1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión ***y,*** ~~especialmente en lo que respecta~~ ***en relación con terceros,*** a ***que estos supriman todos*** los ***enlaces a los*** datos personales ~~proporcionados por el interesado siendo niño~~, ***copias o reproducciones de los mismos,*** cuando concurra alguna de las circunstancias siguientes: a)los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b)el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; c)el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19; ***c bis) un órgano jurisdiccional o una autoridad reguladora con sede en la Unión ha resuelto de forma definitiva e irrevocable que han de suprimirse los datos de que se trate;*** d)~~el tratamiento de~~ ***los*** datos ~~no es conforme con el presente Reglamento por otros motivos~~ ***han sido tratados ilícitamente***. ***1 bis. La aplicación del apartado 1 dependerá de la capacidad del responsable del tratamiento para comprobar que es el interesado quien solicita la supresión de los datos.***	**Artículo 17-** **Derecho de supresión («el derecho al olvido»)** 1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación.	2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales ***sin una justificación basada en el artículo 6***, ***apartado 1***, adoptará todas las medidas razonables~~, incluidas medidas técnicas, en lo que respecta a~~ ***para que*** los datos ***sean suprimidos, también por terceros, sin perjuicio*** de ~~cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos~~ ***lo dispuesto en el artículo 77*** . Cuando ***sea posible,*** el responsable del tratamiento ~~haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación~~ ***informará al interesado de las medidas tomadas por los terceros en cuestión*** .	2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.
3. El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria: a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80; b) por motivos de interés publico en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo 81; c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83; d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida; e) en los casos contemplados en el apartado 4.	3. El responsable del tratamiento ~~procederá~~ ***y, en su caso, el tercero procederán*** a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria: a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80; b) por motivos de interés publico en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo 81; c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83; d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida; e) en los casos contemplados en el apartado 4.	3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones

4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando: a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos; b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios; c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso; d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el artículo 18, apartado 2.	4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales ***, de forma que no sean objeto de las operaciones normales de acceso y tratamiento y no puedan volver a modificarse,*** cuando: a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos; b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios; c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso; ***c bis) un órgano jurisdiccional o una autoridad reguladora con sede en la Unión haya resuelto de forma definitiva e irrevocable que ha de limitarse el tratamiento de los datos de que se trate;*** d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el artículo ~~18, apartado 2.~~ ***15, apartado 2 bis;*** ***d bis) el tipo determinado de tecnología de conservación de los datos no permita su supresión, siempre que dicha tecnología se hubiese puesto en práctica antes de la entrada en vigor del presente Reglamento.*** 5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público. 6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento.	

	~~7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos.~~	
5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público.	8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento.	
6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento.	***8 bis. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de los datos personales, así como para el examen periódico de la necesidad de conservar los datos.***	
7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos.	9. La Comisión estará facultada ***, tras haber solicitado un dictamen al Consejo Europeo de Protección de Datos,*** para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar: a)los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos; b)las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2; c)los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4. **[Enm. 112]**	
8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento.		
9. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar: a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos; b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2; c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.		

ANEXO II

Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS 108)

CURRENT TEXT OF THE CONVENTION AND ADDITIONAL PROTOCOL	MODERNISED CONVENTION 108
Preamble	**Preamble**
The member States of the Council of Europe, signatory hereto,	The member States of the Council of Europe, and the other signatories hereto,
Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;	Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;
Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;	Considering that it is necessary to secure the human dignity and protection of the human rights and fundamental freedoms of every individual and, given the diversification, intensification and globalisation of data processing and personal data flows, personal autonomy based on a person's right to control of his or her personal data and the processing of such data;
Reaffirming at the same time their commitment to freedom of information regardless of frontiers;	Recalling that the right to protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with other human rights and fundamental freedoms, including freedom of expression;
	Considering that this Convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to official documents;
Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,	Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and protection of personal data, thereby contributing to the free flow of information between people;
	Recognising the interest of a reinforcement of international co-operation between the Parties to the Convention,
Have agreed as follows:	Have agreed as follows:
Chapter I – General provisions	**Chapter I – General provisions**
Article 1 – Object and purpose	**Article 1 – Object and purpose**

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").	The purpose of this Convention is to protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.
Article 2 – Definitions	**Article 2 – Definitions**
For the purposes of this Convention:	For the purposes of this Convention:
a "personal data" means any information relating to an identified or identifiable individual ("data subject");	a "personal data" means any information relating to an identified or identifiable individual ("data subject");
b "automated data file" means any set of data undergoing automatic processing;	Deleted
c "automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;	b "data processing" means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;
	c where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;
d "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.	d "controller" means the natural or legal person, public authority, service, agency or any other body which alone or jointly with others has decision-making power with respect to data processing;
	e. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

	f. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
Article 3 – Scope	**Article 3 – Scope**
1 The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.	1 Each Party undertakes to apply this Convention to data processing subject to its jurisdiction in the public and private sectors, thereby securing every individual's right to protection of his or her personal data.
2 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:	2 This Convention shall not apply to data processing carried out by an individual in the course of purely personal or household activities.
a that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;	Deleted
b that it will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;	Deleted
c that it will also apply this Convention to personal data files which are not processed automatically.	Deleted
3 Any State which has extended the scope of this Convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.	Deleted

4 Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this Convention to such categories by a Party which has not excluded them.	Deleted
5 Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2b and c above may not claim the application of this Convention on these points with respect to a Party which has made such extensions.	Deleted
6 The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the Convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.	Deleted
Chapter II – Basic principles for data protection	**Chapter II – Basic principles for the protection of personal data**
Article 4 – Duties of the Parties	**Article 4 – Duties of the Parties**
1 Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.	1 Each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application.
2 These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.	2 These measures shall be taken by each Party and shall have come into force by the time of ratification or of accession to this Convention.
	3 Each Party undertakes: a. to allow the Convention Committee provided for in Chapter VI to evaluate the effectiveness of the measures it has taken in its law to give effect to the provisions of this Convention; and b. to contribute actively to this evaluation process.

Article 5 – Quality of data	**Article 5 – Legitimacy of data processing and quality of data**
	1 Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.
	2 Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.
Personal data undergoing automatic processing shall be:	3 Personal data undergoing processing shall be processed lawfully.
a obtained and processed fairly and lawfully;	
b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;	4 Personal data undergoing processing shall be: a processed fairly and in a transparent manner; b collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;
c adequate, relevant and not excessive in relation to the purposes for which they are stored;	c adequate, relevant and not excessive in relation to the purposes for which they are processed;
d accurate and, where necessary, kept up to date;	d accurate and, where necessary, kept up to date;
e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.	e preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
Article 6 – Special categories of data	**Article 6 – Special categories of data**

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.	1 The processing of: - genetic data; - personal data relating to offences, criminal proceedings and convictions, and related security measures; - biometric data uniquely identifying a person; - personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention. 2 Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.
Article 7 – Data security	**Article 7 – Data security**
Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.	1 Each Party shall provide that the controller, and, where applicable the processor, take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.
	2 Each Party shall provide that the controller notifies, without delay, at least the competent supervisory authority within the meaning of Article 15 of this Convention, of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

	Article 8 – Transparency of processing
	1 Each Party shall provide that the controller informs the data subjects of: (a) his or her identity and habitual residence or establishment; (b) the legal basis and the purposes of the intended processing; (c) the categories of personal data processed; (d) the recipients or categories of recipients of the personal data, if any; and (e) the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data. 2 Paragraph 1 shall not apply where the data subject already has the relevant information.
	3 Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.
Article 8 – Additional safeguards for the data subject	**Article 9 – Rights of the data subject**
Any person shall be enabled:	1 Every individual shall have a right:
a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;	a not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration;
b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;	b to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.	c to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; d to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;
	e to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention;
	f to have a remedy under Article 12 where his or her rights under this Convention have been violated;
	g to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention.
	2 Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.
	Article 10 – Additional obligations
	1 Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.

	2 Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.
	3 Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.
	4 Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor.
Article 9 – Exceptions and restrictions	**Article 11 – Exceptions and restrictions**
1 No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.	1 No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:
2 Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:	Deleted

a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;	a the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
b protecting the data subject or the rights and freedoms of others.	b the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.
3 Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.	2 Restrictions on the exercise of the provisions specified in Articles 8 and 9 may be provided for by law with respect to data processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when there is no recognisable risk of infringement of the rights and fundamental freedoms of data subjects.
	3 In addition to the exceptions allowed for in paragraph 1 of this article, with reference to processing activities for national security and defense purposes, each Party may provide, by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfill such aim, exceptions to Article 4 paragraph 3, Article 14 paragraphs 5 and 6 and Article 15, paragraph 2, litterae a, b, c and d. This is without prejudice to the requirement that processing activities for national security and defense purposes are subject to independent and effective review and supervision under the domestic legislation of the respective Party.
Article 10 – Sanctions and remedies	**Article 12 – Sanctions and remedies**
Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.	Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of the provisions of this Convention.

Article 11 – Extended protection	**Article 13 Extended protection**
None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.	None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.
Chapter III – Transborder data flows	**Chapter III – Transborder flows of personal data**
Article 12 – Transborder flows of personal data and domestic law	**Article 14 - Transborder flows of personal data**
1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.	Deleted
2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.	1 A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the transfer of such data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so, if bound by harmonised rules of protection shared by States belonging to a regional international organisation..

3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:	2 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to this Convention, the transfer of personal data may only take place where an appropriate level of protection based on the provisions of this Convention is secured. 3 An appropriate level of protection can be secured by: a. the law of that State or international organisation, including the applicable international treaties or agreements; or b. ad hoc or approved standardised safeguards provided by legally-binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing.
a insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;	4 Notwithstanding the provisions of the previous paragraphs, each Party may provide that the transfer of personal data may take place if: a the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or b the specific interests of the data subject require it in the particular case; or c prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or d it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.

	5 Each Party shall provide that the competent supervisory authority within the meaning of Article 15 of this Convention is provided with all relevant information concerning the transfers of data referred to in paragraph 3.b and, upon request, paragraphs 4.b and 4.c. 6 Each Party shall also provide that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to condition.
b when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.	Deleted
Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention (Additional Protocol)	Deleted
1 Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.	Deleted
2 By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:	Deleted
a if domestic law provides for it because of:	Deleted
– specific interests of the data subject, or	Deleted
– legitimate prevailing interests, especially important public interests, or	Deleted

b if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.	Deleted
Additional Protocol	**Chapter IV – Supervisory authorities**
Article 1	**Article 15 Supervisory authorities**
1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.	1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the provisions of this Convention.
2 a To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.	2 To this end, such authorities: a shall have powers of investigation and intervention; b shall perform the functions relating to transfers of data provided for under Article 14, notably the approval of standardised safeguards; c shall have powers to issue decisions with respect to violations of the provisions of this Convention and may, in particular, impose administrative sanctions; d shall have the power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of the provisions of this Convention; e shall promote: (i) public awareness of their functions and powers as well as their activities; (ii) public awareness of the rights of data subjects and the exercise of such rights; (iii) awareness of controllers and processors of their responsibilities under this Convention; specific attention shall be given to the data protection rights of children and other vulnerable individuals;
	3 The competent supervisory authorities shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.	4 Each competent supervisory authority shall deal with requests and complaints lodged by data subjects concerning their data protection rights and shall keep data subjects informed of progress.
3 The supervisory authorities shall exercise their functions in complete independence.	5 The supervisory authorities shall act with complete independence and impartiality in performing their duties and exercising their powers and in doing so shall neither seek nor accept instructions.
	6 Each Party shall ensure that the supervisory authorities are provided with the resources necessary for the effective performance of their functions and exercise of their powers. 7. Each supervisory authority shall prepare and publish a periodical report outlining its activities. 8. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information to which they have access, or have had access to, in the performance of their duties and exercise of their powers.
4 Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.	9 Decisions of the supervisory authorities may be subject to appeal through the courts.
	10 The supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity.
5 In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.	Deleted
Chapter IV – Mutual assistance	**Chapter V – Co-operation and mutual assistance**
Article 13 – Co-operation between Parties	**Article 16 – Designation of supervisory authorities**
1 The Parties agree to render each other mutual assistance in order to implement this Convention.	1 The Parties agree to co-operate and render each other mutual assistance in order to implement this Convention.

2 For that purpose:	2 For that purpose:
a each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;	a each Party shall designate one or more supervisory authorities within the meaning of Article 15 of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
b each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.	b each Party which has designated more than one supervisory authority shall specify the competence of each authority in its communication referred to in the previous *littera*.
3 An authority designated by a Party shall at the request of an authority designated by another Party:	Deleted
a furnish information on its law and administrative practice in the field of data protection;	Deleted
b take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.	Deleted
	Article 17 – Forms of co-operation
	1 The supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties and exercise of their powers, in particular by: a providing mutual assistance by exchanging relevant and useful information and co-operating with each other under the condition that, as regards the protection of personal data, all the rules and safeguards of this Convention are complied with; b co-ordinating their investigations or interventions, or conducting joint actions; c providing information and documentation on their law and administrative practice relating to data protection.

	2. The information referred to in paragraph 1 shall not include personal data undergoing processing unless such data are essential for co-operation, or where the data subject concerned has given explicit, specific, free and informed consent to its provision.
	3. In order to organise their co-operation and to perform the duties set out in the preceding paragraphs, the supervisory authorities of the Parties shall form a network.
Article 14 – Assistance to data subjects resident abroad	**Article 18 – Assistance to data subjects**
1 Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this Convention.	1 Each Party shall assist any data subject, whatever his or her nationality or residence, to exercise his or her rights under Article 9 of this Convention.
2 When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.	2 Where a data subject resides on the territory of another Party, he or she shall be given the option of submitting the request through the intermediary of the supervisory authority designated by that Party.
3 The request for assistance shall contain all the necessary particulars, relating inter alia to:	3 The request for assistance shall contain all the necessary particulars, relating *inter alia* to:
a the name, address and any other relevant particulars identifying the person making the request;	a the name, address and any other relevant particulars identifying the data subject making the request;
b the automated personal data file to which the request pertains, or its controller;	b the processing to which the request pertains, or its controller;
c the purpose of the request.	c the purpose of the request.
Article 15 – Safeguards concerning assistance rendered by designated authorities.	**Article 19 – Safeguards**
1 An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.	1 A supervisory authority which has received information from another supervisory authority, either accompanying a request or in reply to its own request shall not use that information for purposes other than those specified in the request.

2 Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.	Deleted
3 In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.	2 In no case may a supervisory authority be allowed to make a request on behalf of a data subject of its own accord and without the express approval of the data subject concerned.
Article 16 – Refusal of requests for assistance	**Article 20 – Refusal of requests**
A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this Convention may not refuse to comply with it unless:	A supervisory authority to which a request is addressed under Article 17 of this Convention may not refuse to comply with it unless:
a the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;	a the request is not compatible with its powers;
b the request does not comply with the provisions of this Convention;	b the request does not comply with the provisions of this Convention;
c compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.	c compliance with the request would be incompatible with the sovereignty, national security or public order of the Party by which it was designated, or with the rights and fundamental freedoms of individuals under the jurisdiction of that Party.
Article 17 – Costs and procedures of assistance	**Article 21 – Costs and procedures**
1 Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.	1. Co-operation and mutual assistance which the Parties render each other under Article 17 and assistance they render to data subjects under Articles 9 and 18 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party making the request.
2 The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.	2 The data subject may not be charged costs or fees in connection with the steps taken on his or her behalf in the territory of another Party other than those lawfully payable by residents of that Party.

3 Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.	3 Other details concerning the co-operation and assistance, relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.
Chapter V – Consultative Committee	**Chapter VI – Convention Committee**
Article 18 – Composition of the committee	**Article 22 – Composition of the committee**
1 A Consultative Committee shall be set up after the entry into force of this Convention.	1 A Convention Committee shall be set up after the entry into force of this Convention.
2 Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.	2 Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.
3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the Convention to be represented by an observer at a given meeting.	3 The Convention Committee may, by a decision taken by a majority of two-thirds of the representatives of the Parties, invite an observer to be represented at its meetings.
	4 Any Party which is not a member of the Council of Europe shall contribute to the funding of the activities of the Convention Committee according to the modalities established by the Committee of Ministers in agreement with that Party.
Article 19 – Functions of the committee	**Article 23 – Functions of the committee**
The Consultative Committee:	The Convention Committee:
a may make proposals with a view to facilitating or improving the application of the Convention;	a may make recommendations with a view to facilitating or improving the application of the Convention;
b may make proposals for amendment of this Convention in accordance with Article 21;	b may make proposals for amendment of this Convention in accordance with Article 25;
c shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 21, paragraph 3;	c shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 25, paragraph 3;
d may, at the request of a Party, express an opinion on any question concerning the application of this Convention.	d may express an opinion on any question concerning the interpretation or application of this Convention;

	e shall prepare, before any new accession to the Convention, an opinion for the Committee of Ministers relating to the level of personal data protection of the candidate for accession and, where necessary, recommend measures to take to reach compliance with the provisions of this Convention;
	f may, at the request of a State or an international organisation, evaluate whether the level of personal data protection the former provides is in compliance with the provisions of this Convention and, where necessary, recommend measures to be taken to reach such compliance;
	g may develop or approve models of standardised safeguards referred to in Article 14;
	h. shall review the implementation of this Convention by the Parties and recommend measures to be taken in the case where a Party is not in compliance with this Convention;
	i shall facilitate, where necessary, the friendly settlement of all difficulties related to the application of this Convention.
Article 20 – Procedure	**Article 24 – Procedure**
1 The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.	1 The Convention Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once a year and in any case when one-third of the representatives of the Parties request its convocation.
2 A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.	Deleted
3 After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.	2 After each of its meetings, the Convention Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of this Convention.
	3 The voting arrangements in the Convention Committee are laid down in the elements for the Rules of Procedure appended to Protocol CETS No. [223].

4 Subject to the provisions of this Convention, the Consultative Committee shall draw up its own Rules of Procedure.	4. The Convention Committee shall draw up the other elements of its Rules of Procedure and establish, in particular, the procedures for evaluation and review referred to in Article 4, paragraph 3, and Article 23, litterae e, f and h on the basis of objective criteria.
Chapter VI – Amendments	**Chapter VII – Amendments**
Article 21 – Amendments	**Article 25 – Amendments**
1 Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.	1 Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Convention Committee.
2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this Convention in accordance with the provisions of Article 23.	2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the Parties to this Convention, to the other member States of the Council of Europe, to the European Union and to every non-member State or international organisation which has been invited to accede to this Convention in accordance with the provisions of Article 28.
3 Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.	3 Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Convention Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
4 The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.	4 The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Convention Committee and may approve the amendment.
5 The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.	5 The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.
6 Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.	6 Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

	7 Moreover, the Committee of Ministers may, after consulting the Convention Committee, decide unanimously that a particular amendment shall enter into force at the expiration of a period of three years from the date on which it has been opened to acceptance, unless a Party notifies the Secretary General of the Council of Europe of an objection to its entry into force. If such an objection is notified, the amendment shall enter into force on the first day of the month following the date on which the Party to this Convention which has notified the objection has deposited its instrument of acceptance with the Secretary General of the Council of Europe.
Chapter VII – Final clauses	**Chapter VIII – Final clauses**
Article 22 – Entry into force	**Article 26 – Entry into force**
1 This Convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.	1 This Convention shall be open for signature by the member States of the Council of Europe and by the European Union. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
2 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.	2 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.
3 In respect of any member State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.	3 In respect of any Party which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.

Article 23 – Accession by non-member States	**Article 27 – Accession by non-member States or international organisations**
1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.	1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, after consulting the Parties to this Convention and obtaining their unanimous agreement, and in light of the opinion prepared by the Convention Committee in accordance with Article 23.e, invite any State not a member of the Council of Europe or an international organisation to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
2 In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.	2 In respect of any State or international organisation acceding to this Convention according to paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.
Article 24 – Territorial clause	**Article 28 – Territorial clause**
1 Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.	1 Any State, the European Union or other international organisation may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
2 Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.	2. Any State, the European Union or other international organisation may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.	3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.
Article 25 – Reservations	**Article 29 – Reservations**
No reservation may be made in respect of the provisions of this Convention.	No reservation may be made in respect of the provisions of this Convention.
Article 26 – Denunciation	**Article 30 – Denunciation**
1 Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.	1 Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
2 Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.	2 Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.
Article 27 – Notifications	**Article 31 – Notifications**
The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this Convention of:	The Secretary General of the Council of Europe shall notify the member States of the Council and any Party to this Convention of:
a any signature;	a any signature;
b the deposit of any instrument of ratification, acceptance, approval or accession;	b the deposit of any instrument of ratification, acceptance, approval or accession;
c any date of entry into force of this Convention in accordance with Articles 22, 23 and 24;	c any date of entry into force of this Convention in accordance with Articles 26, 27 and 28;
d any other act, notification or communication relating to this Convention.	d any other act, notification or communication relating to this Convention.
	Appendix to the Protocol: Elements for the Rules of Procedure of the Convention Committee
	1 Each Party has a right to vote and shall have one vote.

	2 A two thirds majority of representatives of the Parties shall constitute a quorum for the meetings of the Convention Committee. In case the amending Protocol to the Convention enters into force in accordance with its Article 37 paragraph 2 before its entry into force in respect of all Contracting States to the Convention, the quorum for the meetings of the Convention Committee shall be no less than 34 Parties to the Protocol.
	3 The decisions under Article 23 shall be taken by a four-fifths majority. The decisions pursuant to Article 23 littera h shall be taken by a four-fifths majority, including a majority of the votes of States Parties not members of a regional integration organisation that is a Party to the Convention.
	4 Where the Convention Committee takes decisions pursuant to Article 23 littera h, the Party concerned by the review shall not vote. Whenever such a decision concerns a matter falling within the competence of a regional integration organisation, neither the organisation nor its member States shall vote.
	5 Decisions concerning procedural issues shall be taken by a simple majority.
	6 Regional integration organisations, in matters within their competence, may exercise their right to vote in the Convention Committee, with a number of votes equal to the number of their member States that are Parties to the Convention. Such an organisation shall not exercise its right to vote if any of its member States exercises its right.
	7 In case of vote, all Parties must be informed of the subject and time for the vote, as well as whether the vote will be exercised by the Parties individually or by a regional integration organisation on behalf of its member States.
	8 The Convention Committee may further amend its Rules of Procedure by a two-thirds majority, except for the voting arrangements which may only be amended by unanimous vote of the Parties and to which Article 25 of the Convention applies.